# COMPLEX MULTIPLICATION OF ABELIAN SURFACES

PROEFSCHRIFT

ter verkrijging van
de graad van Doctor aan de Universiteit Leiden,
op gezag van Rector Magnificus prof. mr. P.F. van der Heijden,
volgens besluit van het College voor Promoties
te verdedigen op dinsdag 1 juni 2010
klokke 15:00 uur
door

Theodorus Cornelis Streng

geboren te IJsselstein
in 1982

Samenstelling van de promotiecommissie:

**Promotor**

prof. dr. Peter Stevenhagen

**Overige leden**

prof. dr. Gunther Cornelissen (Universiteit Utrecht)
prof. dr. Bas Edixhoven
prof. dr. David R. Kohel (Université de la Méditerranée)
prof. dr. Hendrik W. Lenstra Jr.
dr. Ronald van Luijk

# Complex multiplication of abelian surfaces

Marco Streng

Marco Streng
Complex multiplication of abelian surfaces

ISBN-13 / EAN: 978-90-5335-291-5
AMS subj. class.: 11G15, 14K22
NUR: 921

Thomas Stieltjes Institute
for Mathematics


marco.streng@gmail.com

Typeset using LaTeX
Printed by Ridderprint, Ridderkerk
Asteroids, of which a screen shot is shown on page 188, is due to Atari, 1979.

The cover illustration shows the complex curve $C : y^2 = x^5 + 1$ in the coordinates $(\operatorname{Re} x, \operatorname{Im} x, \operatorname{Re} y)$. Its Jacobian $J(C)$ is an abelian surface with complex multiplication by $\mathbf{Z}[\zeta_5]$ induced by the curve automorphism $\zeta_5 : (x, y) \mapsto (\zeta_5 x, y)$. The colored curves are the real locus of $C$ and its images under $\langle \zeta_5 \rangle$. The illustration was created using Sage [70] and Tachyon.

# Contents

# Introduction

The theory of *complex multiplication* makes it possible to construct certain *class fields* and *abelian varieties*. The main theme of this thesis is making these constructions explicit for the case where the abelian varieties have dimension 2.

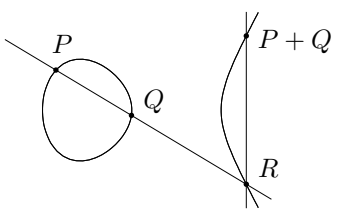
## Elliptic curves over finite fields

One-dimensional abelian varieties are known as *elliptic curves*, which in most cases can be represented as a curve in the $(x, y)$-plane given by

$$y^2 = x^3 + ax + b \tag{0.1}$$

for some choice of parameters $a$, $b$ in a field $k$. Elliptic curves come with a natural (abelian) group law, which can be described completely geometrically.

In the representation (0.1), the unit element of the group is an extra point $O$ at infinity, and three points $P, Q, R$ satisfy $P + Q + R = O$ in the group if and only if they are collinear. For $k = \mathbf{R}$, this looks as follows.




The group law can be given by algebraic equations, and we can define elliptic curves over any field $k$. If $k$ has characteristic different from 2 and 3, which we assume from now on for simplicity, then this is done by taking $a$ and $b$ in $k$. If we do this for a *finite* field $k$, then the group $E(k)$

of points defined over $k$ is finite. Indeed, the number of elements $\#E(k)$ of $E(k)$ can be computed simply by testing for every $x$-coordinate in $k$ whether $x^3 + ax + b$ is a square in $k$.

If the order $q = \#k$ of $k$ gets large, then this method of point counting takes too much time. However, there are faster methods based on the properties of the *Frobenius endomorphism* $F : (x, y) \mapsto (x^q, y^q)$ of $E$. The points in $E(k)$ are exactly those points over an algebraic closure of $k$ that are left invariant by $F$. In particular, they are the points in the kernel of the endomorphism $(F - \mathrm{id})$, where subtraction takes place in the *ring of endomorphisms* $\mathrm{End}(E)$ of $E$. It is known that $F$ is (as an element of the endomorphism ring) a root of a quadratic *Weil polynomial*

$$f = X^2 - tX + q \in \mathbf{Z}[X], \tag{0.2}$$

and that we have

$$\#E(k) = \deg(F - \mathrm{id}) = f(1) = q + 1 - t.$$

The *trace of Frobenius* $t$ is bounded in size by $|t| \leq 2\sqrt{q}$, and indicates to which extent $\#E(k)$ differs from the number $q+1$ of points on a straight line. Schoof realized in 1985 that the reductions $(t \bmod l)$ at small primes $l$ can be computed by looking at the action of $F$ on the $l$-torsion points of $E$, and that this allows one to compute the number $t$, and therefore $\#E(k)$, efficiently. This yields a polynomial time algorithm that, for large $q$, is much faster than the exponential time method of direct point counting.

## Cryptography

Suppose one has a finite group $G$ in which the group operation can be efficiently implemented, but the *discrete logarithm problem* is thought to be hard. This means that given $x, y \in G$, finding an integer $m$ such that $y = x^m$ holds is hard. Then the *Diffie-Hellman key exchange* protocol from 1976 allows one to agree upon a cryptographic key in such a way that eavesdroppers, who intercept the entire communication, are believed to be unable to derive the key from it. The original example of such a group $G$ is the unit group $G = k^*$ for a prime finite field $k = \mathbf{F}_p$. *Index calculus* methods like the *number field sieve* provide a sub-exponential method for solving the discrete logarithm problem in $k^*$. To protect the protocol against this algorithm until the year 2030, it is generally recommended to use primes $p$ of over 3000 bits.

As for $G = k^*$, the group order of $G = E(k)$ for an elliptic curve $E$ is of size approximately $\#k = q$. However, it seems that the discrete logarithm problem for the group $E(k)$ is harder, as 35 years of

research has not led to a sub-exponential method for it. For this reason, the recommended key sizes for achieving the same level of security with *elliptic curve cryptography* are much smaller: $q$ is recommended to have 256 bits. This difference of a factor 12 in key length is important in practical situations such as on 'RFID tags' with limited computing power. The optimal elliptic curves for cryptography are the ones of prime group order, and we will now describe how they can be obtained.

## The CM method

One can construct elliptic curves of prime order over a finite field $k$ by 'random curves and point counting', that is, by taking random $a$'s and $b$'s in $k$ and computing $\#E(k)$ using Schoof's algorithm until one encounters an elliptic curve of prime order.

An alternative method is the *CM method*, which starts with a Weil polynomial $f$ (as in equation (0.2)) with $f(1)$ a large prime, and computes an elliptic curve corresponding to that. Let $\pi$ be a root of $f$ and let $\mathcal{O}$ be the maximal order in the field $\mathbf{Q}(\pi)$. One constructs, e.g. from the torus $\mathbf{C}/\mathcal{O}$ using analytic means, a complex elliptic curve $E$ with *complex multiplication (CM)* by $\mathcal{O}$, i.e., endomorphism ring isomorphic to $\mathcal{O}$. This curve $E$ can be defined over a number field, and its reduction modulo a prime over $p$ has $\pi$ (up to units) as its Frobenius endomorphism.

Actually, instead of the curve $E$ itself, one needs only its *$j$-invariant* $j(E)$, since that completely describes the isomorphism class of $E$ over $\mathbf{C}$. The fact that $E$ can be defined over a number field is reflected by the fact that $j(E)$ is an algebraic number. In fact, it is an algebraic integer, and the CM method computes its minimal polynomial $H_{\mathcal{O}} \in \mathbf{Z}[X]$, called the *Hilbert class polynomial* of $\mathcal{O}$. The reduction of $j(E)$ is obtained by computing a root of $(H_{\mathcal{O}} \bmod p)$, and finding the appropriate curve with that $j$-invariant is easy.

Both methods have various advantages and disadvantages. The bit size of the Hilbert class polynomial $H_{\mathcal{O}}$ grows about linearly with the discriminant of $\mathcal{O}$, so the CM method is restricted to number fields $\mathbf{Q}(\pi)$ of small discriminant. In other words, it is restricted to $p$ and $t$ such that $p^2 - 4t$ is a square times a small integer. The CM method therefore provides partial control over $p$, $t$, and $\#E(k)$, and the interplay between these numbers. This could be compared to random curves and point counting, where one has full control over $p$, but hardly any control over $t$.

From a cryptographic perspective, an advantage of the CM method and the control it provides is the possibility to construct curves for *pairing based cryptography*, which is impossible with random curves.

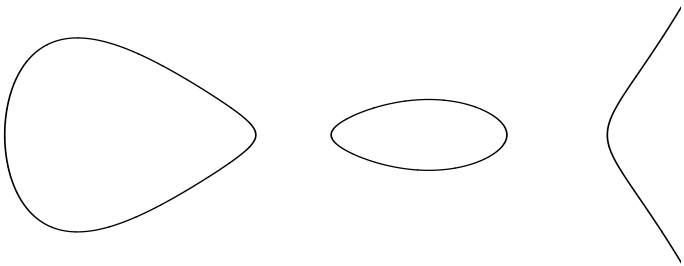
Some cryptographers are a bit hesitant towards curves with too much structure and prefer random curves over the small-discriminant curves produced by the CM method, while others think that special curves might actually be safer than random ones.

## Curves of genus two

Most two-dimensional abelian varieties are *Jacobians* of *curves of genus two*. In characteristic different from 2, curves of genus two are of the form

$$y^2 = f(x)$$

for a polynomial $f$ of degree 5 or 6. This can be compared to equation (0.1) for elliptic curves, where $f$ is a cubic polynomial. Over the field $\mathbf{R}$ of real numbers, this looks for example as follows:



For a curve $C$ of genus 2, the set of *pairs* of points (up to a certain equivalence) has a natural group structure. Three pairs of points add up to the unit element if they lie on the graph of a cubic polynomial. These (classes of) pairs of points form an algebraic surface, an abelian surface known as the *Jacobian* of $C$.

At the moment, the 2-dimensional analogue of Schoof's method, although still polynomial-time, is only just becoming able to construct cryptographic abelian surfaces by 'random curves and point counting'. Analogues of the CM method are much more successful, and various CM constructions for genus 2 have been given during the last two decades. The imaginary quadratic field $\mathbf{Q}(\pi)$ needs to be replaced by a *CM-field* of degree 4, and the $j$-invariant needs to be replaced by a triple of *Igusa invariants*.

The polynomials that one gets instead of Hilbert class polynomials are known as *Igusa class polynomials*. Methods for computing these polynomials were given by Spallek and others, but no bounds on the running time were given. Various complications arise from the facts

that these polynomials are rational, rather than integral, and that the *moduli space* of genus-2 curves is three-dimensional rather than one-dimensional. We study and improve the algorithms in Chapters II and III, and derive the first bound on their running time.

In Chapters IV and V, we describe how to use CM constructions to construct specific kinds of genus-2 curves with Jacobians suitable for cryptography.

## Class fields

Apart from the relatively recent cryptographic applications of CM constructions, the theory of complex multiplication is a beautiful part of pure mathematics that connects number theory, algebra, and geometry.

The *Kronecker-Weber theorem* from the second half of the 19th century states that every finite *abelian* extension $L$ of $\mathbf{Q}$, i.e., every Galois extension $L/\mathbf{Q}$ with finite abelian Galois group, is contained in $\mathbf{Q}(\zeta_n)$ for some $n$, where $\zeta_n$ is a primitive $n$-th root of unity. In other words, every abelian extension $L/\mathbf{Q}$ is a subfield of a field $M$ generated by *torsion elements* $\zeta_n = \exp(2\pi i/n)$ of the group $\mathbf{C}^*$.

The problem of finding similar constructions when $\mathbf{Q}$ is replaced by other base fields $K$ is known as *Kronecker's Jugendtraum* and is number 12 of Hilbert's famous list of 23 problems from the year 1900.

Kronecker found that the $j$-invariants of elliptic curves with CM by orders in an imaginary quadratic field $K$ together with the roots of unity generate almost all abelian extensions of $K$ (indeed, they generate an extension over which the maximal abelian extension has exponent 2). This was later generalized to the theory of *complex multiplication* of elliptic curves, which gives a complete solution to Kronecker's Jugendtraum for $K$ imaginary quadratic. The main theorem of complex multiplication states that for any elliptic curve $E$ with CM by $K$, every finite abelian extension $L/K$ is a subfield of a field $M$ generated by $j(E)$ and the coordinates of torsion points of $E$.

The theory of *complex multiplication of abelian varieties* was developed by Shimura and Taniyama in the 1950's and describes abelian extensions of *CM-fields* $K$. The CM-fields of degree 2 are exactly the imaginary quadratic fields, and this case is the classical case, describing all abelian extensions of imaginary quadratic fields.

For CM-fields $K$ of degree $> 2$, the theory of complex multiplication by itself does *not* produce all abelian extensions of $K$. It does describe which fields are obtained in terms of *class field theory*, and Shimura showed in the 1960's how to obtain all abelian extensions of any CM-field $K$ by using a combination of complex multiplication and the class

fields of the maximal totally real subfield of $K$. For most CM-fields of degree 4, Shimura's construction requires the use of 4-dimensional abelian varieties. We show in Chapter I that it is possible to construct class fields of quartic CM-fields using, besides the class fields of the real quadratic subfield, CM theory only for abelian varieties of dimension at most 2.

## Overview

**Chapter I** is mainly an introduction to the theory of complex multiplication. We define notions that occur in every chapter of this thesis, and we state the 'main theorem' of the theory of complex multiplication. We also show that a general result of Shimura [76] can be improved for the case of CM-fields of degree 4.

**Chapter II** needs only theory from Sections 1–6 of Chapter I and does not require familiarity with class field theory, which Sections I.9 and I.10 do.

We define class polynomials for primitive quartic CM-fields and give an algorithm for computing them. The algorithm is based on an algorithm of Spallek [79] and van Wamelen [88]. We make the algorithm more explicit, and derive the first bounds on the absolute values of the coefficients of the polynomials. Together with recent bounds on the denominators of these coefficients, this provides us with the first running time bound and proof of correctness of an algorithm that computes these polynomials. In fact, no bounds on the height of these polynomials were known yet, so that we also get the first bound on their height.

**Chapter III** shows that there exist better objects than Igusa class polynomials, both from a theoretical perspective and in view of applications. This chapter studies and computes the irreducible components of the modular variety of abelian surfaces with CM by a given primitive quartic CM-field. We show how to adapt the algorithms of Chapter II to compute these irreducible components. We do not do that in Chapter II to avoid making that chapter too heavy, and because Igusa class polynomials are the objects used in existing literature. We also give computational examples in this chapter. Chapter III uses results from both Chapters I and II.

**Chapters IV and V**, which were written to be read independently of each other and of the other chapters, construct certain 'Weil numbers' inside CM-fields. These Weil numbers correspond to abelian varieties,

which in the dimension-2 case can be constructed using the class polynomials of Chapter II. The Weil numbers in Chapters IV and V have properties that are number theoretic in nature and are motivated by cryptography, since the abelian varieties that they correspond to have a subgroup of 'cryptographic' size and hence can be used for cryptographic purposes.

Chapter IV is joint work with David Freeman and Peter Stevenhagen and appeared as *Abelian varieties with prescribed embedding degree* [26]. The abelian varieties in it have a prescribed small 'embedding degree' with respect to a subgroup of large prescribed order. For small dimension, say at most 3, they can be used for 'pairing based cryptography'.

Chapter V is joint work with Laura Hitt O'Connor, Gary McGuire, and Michael Naehrig and appeared as *A CM construction for curves of genus 2 with p-rank 1* [43]. This chapter is about Jacobians of curves of genus 2. The $p$-rank of the abelian surfaces in this chapter, an invariant that is 0 or 2 for all previous cryptographic constructions, is 1.

**Appendices 1–3** give extra background for Chapter II.

Appendix 1 obtains integrality results for Fourier expansions of Igusa invariants directly from formulas in Section II.7.

Appendix 2 gives an alternative to an algorithm in Section II.3 and gives a generalization of much-cited formulas of Spallek [79].

Appendix 3 studies experimentally how fast Igusa class polynomials grow with the discriminant of the CM-field. We also see that our choice of Igusa invariants is better in practice than the invariants used in existing literature.

Chapter I

# Complex multiplication

Abstract. *In this chapter, we give an introduction to the theory of complex multiplication. We define notions like* CM-fields*,* CM-types*, and the* reflex type *that occur in every chapter of this thesis, and we state the 'main theorem' of complex multiplication. We show in Theorem 10.3 that a general result of Shimura [76] can be improved for the case of CM-fields of degree* 4

## 1 Kronecker's Jugendtraum

The following classical result describes all finite abelian extensions of $\mathbf{Q}$ via Galois theory.

**Theorem 1.1** (Kronecker-Weber Theorem)**.** *Let $K/\mathbf{Q}$ be a finite abelian Galois extension. Then there is a positive integer $n$ such that we have an embedding*

$$K \to \mathbf{Q}(\zeta_n) = \mathbf{Q}(t : t \in \mathbf{G}_m(\overline{\mathbf{Q}})[n]) = \mathbf{Q}(\exp(\tfrac{2\pi i}{n})).$$

*The Galois group of $\mathbf{Q}(\zeta_n)/\mathbf{Q}$ is $(\mathbf{Z}/n\mathbf{Z})^*$, where $(k \bmod n)$ maps $\zeta_n$ to $\zeta_n^k$.*

*Kronecker's Jugendtraum* (a.k.a. *Hilbert's twelfth problem*) is to find an analogue of this result when $\mathbf{Q}$ is replaced by an arbitrary number field $F$.

Class field theory *implicitly* describes all finite abelian extensions of $F$ and their Galois groups in terms of certain groups of equivalence classes of ideals. These groups are called *class groups*, and to each class group of $F$, there corresponds an abelian extension of $F$, which we call the *class field* corresponding to the group. The Galois group of an abelian extension of $F$ is isomorphic to the corresponding class group via the *Artin map*.

All class fields can be constructed from their class groups using *Kummer theory*. Suppose we want to construct the finite abelian extension $M$ of $F$ corresponding to a class group $G$. If $e$ is the exponent of $G$, then by Kummer theory, we find that $M$ is a subfield of $F(\zeta_e)(\sqrt[e]{S})$ for some finite set $S \subset F(\zeta_e)$. As the Artin map tells us much about the decomposition of primes in $M/F$, this allows us to find $M$. For details, see Cohen and Stevenhagen [18].

The approach of finding the abelian extensions of $F$ via Kummer theory is arguably not in the spirit of Kronecker's Jugendtraum, since it is not of the form of a single function that parametrizes generators of the abelian extensions of $F$, like the analytic map $z \mapsto \exp(2\pi i z)$ for $F = \mathbf{Q}$.

If $F$ is *imaginary quadratic*, then the theory of complex multiplication of elliptic curves does provide a complete solution to Kronecker's Jugendtraum in terms of the $j$-invariant and the coordinates of torsion points. These torsion points can be parametrized by a normalized version of the Weierstrass $\wp$-function, or 'better' modular functions as in [18]. This approach does not suffer from the need for extra roots of unity $\zeta_e$, as Kummer theory does.

With the theory of complex multiplication of *abelian varieties*, Shimura and Taniyama [78] generalized the full answer for imaginary quadratic fields to a partial answer for *CM-fields*.

For a CM-field $F$, we obtain many abelian extensions of $F$ by replacing $\mathbf{G}_m$ above by an abelian variety that has complex multiplication by the *reflex field* $K$ of $F$. Which abelian extensions are obtained is expressed in terms of the *reflex type*. We will first define these notions.

## 2 CM-fields

**Definition 2.1.** A *CM-field* is a totally imaginary quadratic extension $K$ of a totally real number field $K_0$.

By 'totally imaginary' we mean that $K$ has no embeddings into $\mathbf{R}$. In other words, a CM-field is a field $K = K_0(\sqrt{r})$ for some totally real number field $K_0$ and some totally negative element $r \in K_0$. CM-fields

clearly have even degree, and the CM-fields of degree 2 are exactly the imaginary quadratic number fields.

The following result gives some classical properties of CM-fields.

**Lemma 2.2.** *Let $K$ be a number field. The following are equivalent.*

*(1) The field $K$ is totally real or a CM-field.*

*(2) There exists an automorphism $\bar{\cdot} : x \mapsto \overline{x}$ of $K$ such that for every embedding $\sigma : K \to \mathbf{C}$, the automorphism $\bar{\cdot}$ is the restriction of complex conjugation on $\mathbf{C}$ to $K$ via $\sigma$, i.e., we have $\bar{\cdot} \circ \sigma = \sigma \circ \bar{\cdot}$.*

*Moreover, the following holds:*

*(a) any composite of finitely many CM-fields and totally real fields containing at least one CM-field is a CM-field,*

*(b) the normal closure of a CM-field is a CM-field,*

*(c) if $\phi$ is an embedding of CM-fields $K_1 \to K_2$, then we have $\bar{\cdot} \circ \phi = \phi \circ \bar{\cdot}$ with $\bar{\cdot}$ as in (2),*

*(d) any subfield of a CM-field is totally real or a CM-field.*

Following part (c) of the lemma, we denote $\bar{\cdot} \circ \phi$ by $\overline{\phi}$.

*Proof.* If $K$ is totally real, then (1) and (2) are both trivially true. Otherwise, the equivalence of (1) and (2) follows by taking $K_0$ to be the fixed field of $\bar{\cdot}$. Using (2), we also find (c) since the composite of $\phi$ with an embedding $K_2 \to \mathbf{C}$ is an embedding $K_1 \to \mathbf{C}$. For details, see [52, §I.2], [78, Lemma 3 in §8.1], or [64, Prop. 1.4].

The existence and uniqueness of the complex conjugation morphism $\bar{\cdot}$ of (2) easily shows that a composite of fields satisfying (2) also satisfies (2). In particular, such a composite is a CM-field if one of the fields is a CM-field.

Part (b) follows from (a) as the normal closure is the composite of the conjugates. See also [64, Prop. 1.5].

For part (d), let $K$ be a subfield of $L$, where $L$ satisfies (2) for some automorphism $\bar{\cdot}$. By (b), we can assume without loss of generality that $L$ is normal over $\mathbf{Q}$, so let $H = \mathrm{Gal}(L/K) \subset \mathrm{Gal}(L/\mathbf{Q})$. By (c), we have $\bar{\cdot} \circ H = H \circ \bar{\cdot}$, so $\bar{\cdot}$ restricts to an automorphism of $K$. Since every embedding $K \to \mathbf{C}$ extends to an embedding $L \to \mathbf{C}$, we find that $\bar{\cdot}$ satisfies (2) also on $K$. □

**Example 2.3.** The cyclotomic field $\mathbf{Q}(\zeta_n)$ satisfies (2) for $\overline{\zeta_n} = \zeta_n^{-1}$. It is a CM-field of degree $\varphi(n)$ for $n > 2$ and equals $\mathbf{Q}$ for $n \in \{1, 2\}$. Its totally real subfield is the fixed field $\mathbf{Q}(\zeta_n + \zeta_n^{-1})$ of complex conjugation.

# 3 CM-types

Let $K$ be a CM-field of degree $2g$ and $L'/\mathbf{Q}$ a field that contains a subfield isomorphic to a normal closure of $K$.

**Definition 3.1.** A *CM-type* of $K$ with values in $L'$ is a subset $\Phi \subset \mathrm{Hom}(K, L')$ consisting of exactly one element from each of the $g$ *complex conjugate pairs* of embeddings $\phi, \overline{\phi} : K \to L'$.

There are $2^g$ CM-types of $K$ with values in $L'$. If $K$ is imaginary quadratic, then a CM-type of $K$ with values in $L'$ is the same as an embedding of $K$ into $L'$.

Let $K_2/K_1$ be an extension of CM-fields and assume $L'$ contains a subfield isomorphic to a normal closure of $K_2$. Then every CM-type of $K_1$ has a natural extension to a CM-type of $K_2$ as follows.

**Definition 3.2.** Let $K_1, K_2, L'$ be as above, and let $\Phi$ be a CM-type of $K_1$ with values in $L'$. The CM-type of $K_2$ *induced* by $\Phi$ is

$$\Phi_{K_2} = \{\phi \in \mathrm{Hom}(K_1, L') : \phi_{|K_1} \in \Phi\}.$$

We say that a CM-type is *primitive* if it is not induced from a CM-type of a strict CM-subfield.

**Example 3.3.** The cyclic CM-field $K = \mathbf{Q}(\zeta_7)$ of degree 6 has subfields $K_0 = \mathbf{Q}(\zeta_7 + \zeta_7^{-1})$, $K_1 = \mathbf{Q}(\sqrt{-7})$, and $\mathbf{Q}$. We see that $K$ has $2^3 = 8$ CM-types of which 2 are induced from $K_1$, hence 6 CM-types are primitive.

We call two CM-types $\Phi_1, \Phi_2$ of $K$ *equivalent* if there is an automorphism $\sigma$ of $K$ such that $\Phi_2 = \Phi_1\sigma$ holds.

**Lemma 3.4** (Example 8.4(2) of [78])**.** *Let $K$ be a quartic CM-field with the four distinct embeddings $\phi_1$, $\phi_2$, $\overline{\phi_1}$, $\overline{\phi_2}$ into a field $L'$, and let $\Phi = \{\phi_1, \phi_2\}$, $\Phi' = \{\phi_1, \overline{\phi_2}\}$. Exactly one of the following holds.*

1. *The field $K$ is normal over $\mathbf{Q}$ and its Galois group is isomorphic to $C_2 \times C_2$. Each CM-type is non-primitive, and there are two equivalence classes of CM-types $\{\Phi, \overline{\Phi}\}$ and $\{\Phi', \overline{\Phi'}\}$, where each class is induced from a different imaginary quadratic subfield of $K$.*

2. *The field $K$ is cyclic Galois, and all four CM-types are equivalent and primitive.*

3. *The field $K$ is non-Galois, its normal closure has Galois group $D_4$, each CM-type is primitive, and the equivalence classes of CM-types are $\{\Phi, \overline{\Phi}\}$ and $\{\Phi', \overline{\Phi'}\}$.*

*In cases 2 and 3, the field $K$ does not contain an imaginary quadratic subfield.*

*Proof.* Let $L$ be the normal closure of $K$ and $\mathrm{Gal}(L/\mathbf{Q})$ its Galois group. Then $\mathrm{Gal}(L/\mathbf{Q})$ is a group of permutations of $V = \{\phi_1, \phi_2, \overline{\phi_1}, \overline{\phi_2}\}$ that commute with the complex conjugation permutation. If we identify $V$ with the vertices of a square in the plane, where the complex conjugate elements of $V$ are opposite corners, then $\mathrm{Gal}(L/\mathbf{Q})$ is a subgroup of the symmetry group $D_4$ of the square. The three conjugacy classes of subgroups that act transitively on the vertices are listed in the lemma. For each, the subfields and the equivalence classes of CM-types are straightforward to compute. □

In particular, for a quartic CM-field, either all or none of the CM-types are primitive and we call the field *primitive* or *non-primitive* accordingly. A quartic CM-field is primitive if and only if it does not contain an imaginary quadratic subfield.

The following result shows that every CM-type is induced from a unique CM-subfield.

**Lemma 3.5.** *Let $K$ be a CM-field and $\Phi$ a CM-type of $K$ with values in $L'$. There is a unique subfield $K_1 \subset K$ and a unique CM-type $\Phi_1$ of $K_1$ with values in $L'$ such that $\Phi_1$ is primitive and $\Phi$ is induced from $\Phi_1$.*

*If $L$ is the normal closure of $K$, then we have*

$$\mathrm{Gal}(L/K_1) = \{\sigma \in \mathrm{Gal}(L/\mathbf{Q}) \mid \Phi_L \sigma = \Phi_L\}. \tag{3.6}$$

*Proof.* This is [64, Prop. 1.9] or, alternatively, [52, Lem. 2.2]. □

# 4 Complex multiplication

We now recall the basic theory of abelian varieties with complex multiplication. For details, we refer to [78, 52, 64].

An *abelian variety* over a field $k$ is a complete irreducible group variety over $k$. It is known that abelian varieties are smooth, projective, and commutative.

A *morphism* of abelian varieties is a morphism of varieties that respects the group structure, and we will denote the ring of endomorphisms of an abelian variety $A$ by $\mathrm{End}(A)$. An *isogeny* is a surjective homomorphism between two abelian varieties of the same dimension. We say that $A$ and $B$ are *isogenous* and write $A \sim B$ if there exists an isogeny from $A$ to $B$. This defines an equivalence relation, and we call

a non-zero abelian variety $A$ *simple* if it is not isogenous to a product of lower-dimensional abelian varieties.

We say that an abelian variety $A$ of dimension $g$ has *complex multiplication (CM)* by a number field $M$ if $M$ has degree $2g$ and there is an embedding $\iota : M \to \mathrm{End}(A) \otimes \mathbf{Q}$. We say that $A$ has CM by an order $\mathcal{O} \subset M$ if the same holds with $\iota^{-1}(\mathrm{End}(A)) = \mathcal{O}$.

The *tangent space* $T_0A$ of $A$ at the unit point 0 of $A$ is a vector space over $k$ of dimension $g$. Differentiation defines a ring homomorphism $D : \mathrm{End}(A) \to \mathrm{End}_k(T_0A)$.

Now let $K$ be a CM-field of degree $2g$ and $A$ an abelian variety with CM by $K$ via the embedding $\iota : K \to \mathrm{End}(A) \otimes \mathbf{Q}$. Suppose the base field $k$ has characteristic 0. Then the composite map

$$\rho = D \circ \iota : K \to \mathrm{End}_k T_0A$$

is a $g$-dimensional $k$-linear representation of the ring $K$.

**Lemma 4.1.** *Let the notation be as above, and assume that the base field $k$ has characteristic 0. There exists a unique CM-type $\Phi$ of $K$ with values in the algebraic closure $\overline{k}$ of $k$ such that the representation $\rho$ is equivalent over $\overline{k}$ to the direct sum representation $\oplus_{\phi\in\Phi}\phi$.*

*Proof.* See [78, §5.2], [52, Thm. 1.3.4], or [64, 3.11]. □

The CM-type $\Phi$ is uniquely determined by $(A, \iota)$ and we call it *the CM-type of* $(A, \iota)$. Furthermore, we say that $(A, \iota)$ and $A$ are *of type* $\Phi$. Note that if $\sigma$ is an automorphism of $K$ and $(A, \iota)$ is of type $\Phi$, then $(A, \iota \circ \sigma)$ is of type $\Phi \circ \sigma$. In particular, the variety $A$ is both of type $\Phi$ and of type $\Phi \circ \sigma$.

Given any element $\tau \in \mathrm{Gal}(\overline{k}/\mathbf{Q})$, we define

$$\begin{aligned} \tau\iota : K &\to \mathrm{End}(\tau A) \otimes \mathbf{Q} \\ x &\mapsto \tau(\iota(x)). \end{aligned}$$

We write $\tau(A, \iota) = (\tau A, \tau\iota)$.

**Lemma 4.2.** *With $\tau$ as above, if $(A, \iota)$ has type $\Phi$, then $\tau(A, \iota)$ has type $\tau\Phi$.*

*Proof.* Follows directly from the definition. See also the proof of Proposition 31 in §8.5 of [78]. □

The *reflex field* $K^{\mathrm{r}} \subset \overline{k}$ of $(K, \Phi)$ is the fixed field of the group

$$G = \{\tau \in \mathrm{Gal}(\overline{k}/\mathbf{Q}) : \tau\Phi = \Phi\}.$$

We find that for any CM-type $(K, \Phi)$, the group $G = \mathrm{Gal}(\overline{k}/K^{\mathrm{r}})$ acts on the set of abelian varieties of type $\Phi$. The main theorem of complex multiplication, which we will state later, describes this action.

In what follows, we will actually work with *polarized* abelian varieties, which are abelian varieties together with some extra data called a *polarization*. We give the definition of a polarization for a *complex* abelian variety in Section 5.1. We will not need the general definition of a polarization in this thesis, but see [62, §13] for details.

# 5 Complex abelian varieties

## 5.1 Complex tori and polarizations

If $A$ is a $g$-dimensional abelian variety over the field $\mathbf{C}$ of complex numbers, then it is known that there exists a natural complex analytic group homomorphism from the tangent space $V = T_0A$ to $A$. Its kernel $\Lambda$ is a lattice of rank $2g$. This shows that every complex abelian variety is complex analytically a *complex torus*, i.e., a complex vector space modulo a lattice of full rank. A polarization of $A$ induces an anti-symmetric $\mathbf{R}$-bilinear form

$$E : V \times V \to \mathbf{R}$$

such that we have $E(\Lambda, \Lambda) \subset \mathbf{Z}$ and such that $(u, v) \mapsto E(iu, v)$ is symmetric and positive definite. By a *polarization* on a complex torus, we will mean such a form.

A complex torus $V/\Lambda$ is (complex analytically isomorphic to) an abelian variety if and only if it admits a polarization (see [4]).

The derivative of any morphism $f : A \to B$ of abelian varieties is a *morphism of complex tori*, i.e., a $\mathbf{C}$-linear map of the complex vector spaces that restricts to a map of the lattices. Conversely, any morphism of tori $T_0A/\Lambda_A \to T_0B/\Lambda_B$ induces a morphism of abelian varieties. In particular, the category of abelian varieties over $\mathbf{C}$ is equivalent to the category of complex tori that admit a polarization.

The *degree* of a polarization is the determinant $\det M$ of a matrix $M$ that expresses $E$ in terms of a basis of $\Lambda$. We call a polarization *principal* if its degree is 1, and a *(principally) polarized abelian variety* is a pair consisting of an abelian variety together with a (principal) polarization.

An *isomorphism* $f : (\mathbf{C}^g/\Lambda, E) \to (\mathbf{C}^g/\Lambda', E')$ of (principally) polarized abelian varieties is a $\mathbf{C}$-linear isomorphism $f : \mathbf{C}^g \to \mathbf{C}^g$ such that $f(\Lambda) = \Lambda'$ and $f^*E' = E$ hold, where $f^*E'$ is defined by $f^*E'(u, v) = E(f(u), f(v))$ for all $u, v \in \mathbf{C}^g$.

## 5.2 Ideals and polarizations

Let $K$ be any CM-field of degree $2g$ and let $\Phi = \{\phi_1, \ldots, \phi_g\}$ be a CM-type of $K$ with values in $\mathbf{C}$. By abuse of notation, we interpret $\Phi$ as a map $\Phi : K \to \mathbf{C}^g$ by setting $\Phi(\alpha) = (\phi_1(\alpha), \ldots, \phi_g(\alpha)) \in \mathbf{C}^g$ for $\alpha \in K$.

Let $\mathcal{D}_{K/\mathbf{Q}}$ be the different of $K$. Let $\mathfrak{a}$ be a fractional $\mathcal{O}_K$-ideal, and suppose that there exists a generator $\xi \in K$ of the fractional $\mathcal{O}_K$-ideal $(\mathfrak{a}\overline{\mathfrak{a}}\mathcal{D}_{K/\mathbf{Q}})^{-1}$ such that $\phi(\xi)$ lies on the positive imaginary axis for every $\phi \in \Phi$. Then the map $E = E_{\Phi,\xi} : \Phi(K) \times \Phi(K) \to \mathbf{Q}$ given by

$$E(\Phi(\alpha), \Phi(\beta)) = \mathrm{Tr}_{K/\mathbf{Q}}(\xi\overline{\alpha}\beta) \quad \text{for } \alpha, \beta \in K \tag{5.1}$$

is integer valued on $\Phi(\mathfrak{a}) \times \Phi(\mathfrak{a})$, and can be extended uniquely $\mathbf{R}$-linearly to an $\mathbf{R}$-bilinear form $E = E_{\Phi,\xi} : \mathbf{C}^g \times \mathbf{C}^g \to \mathbf{R}$.

**Theorem 5.2.** *Suppose $\Phi$ is a CM-type of a CM-field $K$ of degree $2g$. Then the following holds.*

1. *For any triple $(\Phi, \mathfrak{a}, \xi)$ as above, the pair $(\mathbf{C}^g/\Phi(\mathfrak{a}), E)$ defines a principally polarized abelian variety $A(\Phi, \mathfrak{a}, \xi)$ with CM by $\mathcal{O}_K$ of type $\Phi$.*

2. *Every principally polarized abelian variety over $\mathbf{C}$ with CM by $\mathcal{O}_K$ of type $\Phi$ is isomorphic to $A(\Phi, \mathfrak{a}, \xi)$ for some triple $(\Phi, \mathfrak{a}, \xi)$ as in part 1.*

3. *The abelian variety $A(\Phi, \mathfrak{a}, \xi)$ is simple if and only if $\Phi$ is primitive. If this is the case, then the embedding $\iota : K \to \mathrm{End}(A) \otimes \mathbf{Q}$ is an isomorphism.*

4. *For every pair of triples $(\Phi, \mathfrak{a}, \xi)$ and $(\Phi, \mathfrak{a}', \xi')$ as above with the same type $\Phi$, the principally polarized abelian varieties $A(\Phi, \mathfrak{a}, \xi)$ and $A(\Phi, \mathfrak{a}', \xi')$ are isomorphic if there exists $\gamma \in K^*$ such that*

   *(a) $\mathfrak{a}' = \gamma\mathfrak{a}$ and*

   *(b) $\xi' = (\gamma\overline{\gamma})^{-1}\xi$.*

   *If $\Phi$ is primitive, then the converse holds.*

*Proof.* This result can be derived from Shimura-Taniyama [78], and first appeared in a form similar to the above in Spallek [79, Sätze 3.13, 3.14, 3.19] We quickly give a proof. See van Wamelen [88, Thms. 1, 3, 5] for details.

A straightforward calculation shows that $E$ is anti-symmetric and that $(u, v) \mapsto E(iu, v)$ is symmetric and positive definite (see [78, Thm. 4

in §6.2]). The fact that $E : \Phi(\mathfrak{a}) \times \Phi(\mathfrak{a}) \to \mathbf{Q}$ takes values in $\mathbf{Z}$ and has determinant 1 follows from the fact that $\xi\overline{\mathfrak{a}}\mathfrak{a} = \mathcal{D}_{K/\mathbf{Q}}^{-1}$ is the dual of $\mathcal{O}_K$ for the *trace form* $K \times K \to \mathbf{Z}$ given by $(x, y) \mapsto \mathrm{Tr}_{K/\mathbf{Q}}(xy)$. This proves part 1.

Now let $(A, \iota)$ have type $\Phi$. By definition of the type of $(A, \iota)$ we can choose a basis of $T_0 A$ such that $\iota(\alpha)$ is given by the diagonal matrix with diagonal $\Phi(\alpha)$. Take any element $x \in \Lambda$ and scale the basis of $T_0 A$ such that we have $x = (1, \ldots, 1)$. As $\Lambda$ is an $\mathcal{O}_K$-module via $\Phi$, we find that $\Lambda \otimes \mathbf{Q}$ is a vector space over $K$ via $\Phi$. The dimension of this vector space is $(2g)/(2g) = 1$, so $\Phi^{-1}(\Lambda) \subset K$ is a fractional $\mathcal{O}_K$-ideal, which we denote by $\mathfrak{a}$.

For the details of why a polarization of $(A, \iota)$ takes the form of (5.1), see [78, Thm. 4 in §6.2]. The identity $\xi\overline{\mathfrak{a}}\mathfrak{a} = \mathcal{D}_{K/\mathbf{Q}}^{-1}$ follows from the fact that $E$ maps $\Phi(\mathfrak{a}) \times \Phi(\mathfrak{a})$ to $\mathbf{Z}$ with determinant 1. This proves part 2

The fact that an abelian variety of type $\Phi$ is simple if and only if $\Phi$ is primitive is [52, Thm. 1.3.5]. It then follows from [52, Thm. 1.3.3] that $\iota$ is bijective.

Theorem 5 of [88] gives the condition for when abelian varieties are isomorphic. □

We call two triples $(\Phi, \mathfrak{a}, \xi)$ with the same type $\Phi$ *equivalent* if they satisfy the conditions *4a* and *4b* of Theorem 5.2.

Let $K$ be any CM-field with maximal totally real subfield $K_0$. Let $h$ (resp. $h_0$) be the class number of $K$ (resp. $K_0$) and let $h_1 = h/h_0$.

**Proposition 5.3.** *The number of pairs $(\Phi, A)$, where $\Phi$ is a CM-type and $A$ is an isomorphism class of abelian varieties over $\mathbf{C}$ with CM by $\mathcal{O}_K$ of type $\Phi$, is*

$$h_1 \cdot \#\mathcal{O}_{K_0}^* / N_{K/K_0}(\mathcal{O}_K^*).$$

*Proof.* Let $I$ be the group of invertible $\mathcal{O}_K$-ideals and $S$ the set of pairs $(\mathfrak{a}, \xi)$ with $\mathfrak{a} \in I$ and $\xi \in K^*$ such that $\xi^2$ is totally negative and $\xi\mathcal{O}_K = (\mathfrak{a}\overline{\mathfrak{a}}\mathcal{D}_{K/\mathbf{Q}})^{-1}$. The group $K^*$ acts on $S$ via $x(\mathfrak{a}, \xi) = (x\mathfrak{a}, x^{-1}\overline{x}^{-1}\xi)$ for $x \in K^*$. By Theorem 5.2, the set that we need to count is in bijection with the set $K^*\backslash S$ of orbits.

We claim first that $S$ is non-empty. Proof of the claim: Let $z \in K^*$ be such that $z^2$ is a totally negative element of $K_0$. The norm map $N_{K/K_0} : \mathrm{Cl}(K) \to \mathrm{Cl}(K_0)$ is surjective by [91, Thm. 10.1] and the fact that the infinite primes ramify in $K/K_0$. As $\mathcal{D}_{K/\mathbf{Q}}$ and $x\mathcal{O}_K$ are invariant under complex conjugation, surjectivity of $N$ implies that there exist an element $y \in K_0^*$ and a fractional $\mathcal{O}_K$-ideal $\mathfrak{a}_0$ such that $y\mathfrak{a}_0\overline{\mathfrak{a}_0} = z^{-1}\mathcal{D}_{K/\mathbf{Q}}^{-1}$ holds, so $(\mathfrak{a}_0, yz)$ is an element of $S$.

Let $S'$ be the group of pairs $(\mathfrak{b}, u)$, consisting of a fractional $\mathcal{O}_K$-ideal $\mathfrak{b}$ and a totally positive generator $u \in K_0^*$ of $\mathfrak{b}\overline{\mathfrak{b}}$. The group $K^*$ acts on $S'$ via $x(\mathfrak{b}, u) = (x\mathfrak{b}, x\overline{x}u)$ for $x \in K^*$, and we denote the group of orbits by $C = K^*\backslash S'$. The map $C \to K^*\backslash S : (\mathfrak{b}, u) \mapsto (\mathfrak{b}\mathfrak{a}_0, u^{-1}yz)$ is a bijection and the sequence

$$0 \longrightarrow \mathcal{O}_{K_0}^*/N_{K/K_0}(\mathcal{O}_K^*) \underset{u\mapsto(\mathcal{O}_K,u)}{\longrightarrow} C \underset{(\mathfrak{b},u)\mapsto\mathfrak{b}}{\longrightarrow} \mathrm{Cl}(K) \underset{N}{\longrightarrow} \mathrm{Cl}(K_0) \longrightarrow 0$$

is exact, so $K^*\backslash S$ has the correct order. □

The following two lemmas show what happens with distinct CM-types and thus answers a question of van Wamelen [88].

**Lemma 5.4.** *For any triple $(\Phi, \mathfrak{a}, \xi)$ as above and $\sigma \in \mathrm{Aut}(K)$, we have*

$$A(\Phi, \mathfrak{a}, \xi) \cong A(\Phi \circ \sigma, \sigma^{-1}(\mathfrak{a}), \sigma^{-1}(\xi)).$$

*Proof.* We find twice the same complex torus $\mathbf{C}^g/\Phi(\mathfrak{a})$. The first has polarization

$$E : (\Phi(\alpha), \Phi(\beta)) \mapsto \mathrm{Tr}_{K/\mathbf{Q}}(\xi\overline{\alpha}\beta) \tag{5.5}$$

for $\alpha, \beta \in \mathfrak{a}$ while the polarization of the second maps $(\Phi(\alpha), \Phi(\beta))$ to $\mathrm{Tr}_{K/\mathbf{Q}}(\sigma^{-1}(\xi\overline{\alpha}\beta))$, which equals the right hand side of (5.5). □

**Lemma 5.6.** *Suppose $A$ and $B$ are abelian varieties over $\mathbf{C}$ with CM by $K$ of types $\Phi$ and $\Phi'$. If $\Phi'$ is primitive and $\Phi$ and $\Phi'$ are not equivalent, then $A$ and $B$ are not isogenous. In particular, they are not isomorphic.*

*Proof.* Suppose $f : A \to B$ are isogenous. The isogeny induces an isomorphism $\varphi : \mathrm{End}(A) \otimes \mathbf{Q} \to \mathrm{End}(B) \otimes \mathbf{Q}$ given by $g \mapsto fgf^{-1}$. Let $\iota_A : K \to \mathrm{End}(A) \otimes \mathbf{Q}$ and $\iota_B : K \to \mathrm{End}(B) \otimes \mathbf{Q}$ be the embeddings of types $\Phi$ and $\Phi'$. Let $\sigma = \iota_B^{-1}\varphi\iota_A$ (where $\iota_B$ is an isomorphism by Theorem 5.2.3 because $\Phi'$ is primitive). Then $(A, \iota_A)$ and $(B, \iota_B \circ \sigma)$ have types $\Phi$ and $\Phi'\sigma$. As $f$ induces an isomorphism of the tangent spaces, we also see that these types are equal, so $\Phi$ and $\Phi'$ are equivalent. □

**Definition 5.7.** We call two triples $(\Phi, \mathfrak{a}, \xi)$ and $(\Phi', \mathfrak{a}', \xi')$ *equivalent* if there is an automorphism $\sigma \in \mathrm{Aut}(K)$ such that $\Phi \circ \sigma = \Phi'$ holds and $(\Phi, \sigma(\mathfrak{a}'), \sigma(\xi'))$ is equivalent to $(\Phi, \mathfrak{a}, \xi)$ as in our definition above Lemma 5.4.

If $\Phi$ is primitive, then it follows from Theorem 5.2.4 and Lemmas 5.4 and 5.6 that $A(\Phi, \mathfrak{a}, \xi)$ and $A(\Phi', \mathfrak{a}', \xi')$ are isomorphic if and only if $(\Phi, \mathfrak{a}, \xi)$ and $(\Phi', \mathfrak{a}', \xi')$ are equivalent.

## 5.3 Another representation of the ideals

Let $K$ be any CM-field of degree $2g$ and assume $g \leq 2$, or, more generally, that the different $\mathcal{D}_{K_0/\mathbf{Q}}$ is principal and generated by $\delta \in K_0$. For $g = 1$ we take $\delta = 1$, and for $g = 2$ we take $\delta = \sqrt{\Delta_0}$.

We will now show that we can take the triple $(\Phi, \mathfrak{a}, \xi)$ to be of a special form. This special form is important to us in Section II.6, where we use it to give bounds on the absolute values of matrices occurring in our algorithm.

**Theorem 5.8.** *Let $K$ be a CM-field and $K_0$ its maximal real subfield and suppose that $\mathcal{D}_{K_0/\mathbf{Q}}$ is principal and generated by $\delta$.*

*For every triple $(\Phi, \mathfrak{a}, \xi)$ as in Section 5.2, there exists an element $z \in K$ such that (up to equivalence of the triple $(\Phi, \mathfrak{a}, \xi)$) we have $\mathfrak{a} = z\mathcal{O}_{K_0} + \mathcal{O}_{K_0} \subset K$, $\xi = (z - \overline{z})^{-1}\delta^{-1}$, and $\Phi = \{\phi : K \to \mathbf{C} \mid \operatorname{Im} \phi\xi > 0\}$.*

*Proof.* As $\mathfrak{a}$ is a projective module of rank 2 over the Dedekind domain $\mathcal{O}_{K_0}$, we can write it as $\mathfrak{a} = z\mathfrak{c} + y\mathcal{O}_{K_0}$ for some $\mathcal{O}_{K_0}$-ideal $\mathfrak{c}$ and $z, y \in K$. By part 4 of Theorem 5.2, we can replace $\mathfrak{a}$ by $y^{-1}\mathfrak{a}$ and $\xi$ by $y\overline{y}\xi$, hence we can assume without loss of generality that we have $y = 1$.

Recall that we have an alternating $\mathbf{Z}$-bilinear form $E : \mathfrak{a} \times \mathfrak{a} \to \mathbf{Z}$, given by $(u, v) \mapsto \operatorname{Tr}_{K/\mathbf{Q}}(\xi u\overline{v})$. This form is trivial on $z\mathfrak{c} \times z\mathfrak{c}$ and $\mathcal{O}_{K_0} \times \mathcal{O}_{K_0}$, and is alternating, hence is completely defined by its action on $z\mathfrak{c} \times \mathcal{O}_{K_0}$. Let $T : K_0 \times K_0 \to \mathbf{Q}$ be the $\mathbf{Q}$-linear *trace form* $(a, b) \mapsto \operatorname{Tr}_{K_0/\mathbf{Q}}(ab)$, so we have $E(za, b) = T(\xi(z - \overline{z})a, b)$ for all $a \in \mathfrak{c}, b \in \mathcal{O}_{K_0}$. Note that here $\xi(z - \overline{z})$ is an element of $K_0$.

The fact that $E$ is principal (i.e., has determinant 1) implies that $\xi(z - \overline{z})\mathfrak{c}$ is the dual of $\mathcal{O}_{K_0}$ with respect to the form $T$, which is $\mathcal{D}^{-1}_{K_0/\mathbf{Q}} = \delta^{-1}\mathcal{O}_{K_0}$ by [66, §III.2]. It follows that $\mathfrak{c}$ is principal, so without loss of generality we have $\mathfrak{c} = \mathcal{O}_{K_0}$ and hence $\xi = (z - \overline{z})^{-1}\delta^{-1}$. □

The following result gives the converse of Theorem 5.8. In fact, it gives a slightly more general representation that will be useful in Section II.6.

**Theorem 5.9.** *Let $K$, $K_0$, and $\delta$ be as mentioned at the beginning of Section 5.3.*

*Suppose $z \in K$ is such that $\mathfrak{a} = z\mathfrak{b} + \mathfrak{b}^{-1}$ is an $\mathcal{O}_K$-submodule of $K$. Let $\xi = (z - \overline{z})^{-1}\delta^{-1}$ and $\Phi = \{\phi : K \to \mathbf{C} : \operatorname{Im} \phi\xi > 0\}$. Then $(\Phi, \mathfrak{a}, \xi)$ is a triple as in Section 5.2.*

*Proof.* The dual of $\mathfrak{b}$ for the trace form (as defined in the proof of Theorem 5.8) is $\delta^{-1}\mathfrak{b}^{-1}$. The result now follows by retracing the steps in the proof of Theorem 5.8. □

We call two pairs $(z, \mathfrak{b})$ *equivalent* if they give rise to equivalent triples $(\Phi, \mathfrak{a}, \xi)$.

**Remark 5.10.** The element $z \in K$ can be interpreted as a point

$$-(\mathrm{sign}(\phi_i\delta)\phi_i z)_{i=1}^g$$

in the *Hilbert upper half space* $\mathcal{H}^g$, which is the $g$-fold cartesian product of the upper half plane $\mathcal{H} = \{z \in \mathbf{C} \mid \mathrm{Im}\, z > 0\}$.

The group $\mathrm{SL}_2(\mathcal{O}_{K_0})$ acts on $\mathcal{H}^g$ by acting on the $i$-th coordinate $z_i$ of $z \in \mathcal{H}^g$ as

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} z_i = \frac{\phi_i(a)z_i + \phi_i(b)}{\phi_i(c)z_i + \phi_i(d)}.$$

The *Hilbert moduli space* $\mathrm{SL}_2(\mathcal{O}_{K_0})\backslash\mathcal{H}^g$ parametrizes the set of isomorphism classes of principally polarized abelian varieties with *real multiplication* by $\mathcal{O}_{K_0}$, of which principally polarized abelian varieties with complex multiplication by $\mathcal{O}_K$ are special cases.

# 6 Jacobians of curves

An important example of a principally polarized abelian variety is the *Jacobian* of a curve. By *curve*, we will always mean a smooth projective geometrically irreducible algebraic curve over a field. The Jacobian of a curve $C$ over a field $k$ is an abelian variety $J(C)$ such that we have $J(C)(l) = \mathrm{Pic}^0(C_l)$ for every field extension $l/k$ with $C(l) \neq \emptyset$. For the exact definition or more details, see [63]. The dimension of $J(C)$ equals the genus $g$ of $C$.

If we fix a divisor $E$ of degree $g$ on $C$, then by the Riemann-Roch theorem, every degree-0 divisor on $C$ is equivalent to $D - E$ for an effective divisor $D$ of $C$ of degree $g$, i.e., for a sum $D$ of $g$ points. This gives a cover of $J(C)$ by the $g$-fold symmetric product of $C$, and shows that we can view $J(C)$ as a set of equivalence classes of $g$-tuples of points.

The Jacobian comes with a natural principal polarization. For details, see [63]. We say that a curve $C$ has *complex multiplication* if $J(C)$ does.

Now suppose $C$ is defined over $k = \mathbf{C}$. We give the definition of the Jacobian as in [4]. Let $H^0(\omega_C)$ be the complex vector space of holomorphic 1-forms on $C$ and denote its dual by $H^0(\omega_C)^*$. The homology group $H_1(C, \mathbf{Z})$ is a free abelian group of rank $2g$, and we get a canonical injection $H_1(C, \mathbf{Z}) \to H^0(\omega_C)^*$, given by $\gamma \mapsto (\omega \mapsto \int_\gamma \omega)$, where the integral is taken over any representative cycle of the class $\gamma \in H_1(C, \mathbf{Z})$. The

image of $H_1(C, \mathbf{Z})$ in $H^0(\omega_C)^*$ is a lattice of rank $2g$ in a $g$-dimensional complex vector space, and the quotient $J(C) = H^0(\omega_C)^*/H_1(C, \mathbf{Z})$, which is a complex torus, is the Jacobian of $C$.

**Example 6.1** (Example 15.4(2) of [78])**.** Let $l$ be an odd prime number and consider the field $K = \mathbf{Q}(\zeta)$ for a primitive $l$-th root of unity $\zeta$. Then $K$ is a CM-field of degree $l-1$ and we let $g = (l-1)/2$. Let $C$ be the smooth projective curve of genus $g$ over $\mathbf{C}$ with an affine model

$$y^2 = x^l + 1.$$

There is an isomorphism $\iota : \mathcal{O}_K = \mathbf{Z}[\zeta] \to \mathrm{End}(J(C))$, where $\iota(\zeta)$ is induced by

$$((x, y) \mapsto (\zeta x, y)) \in \mathrm{Aut}(C).$$

The space of holomorphic differentials $H^0(\omega_C)$ of $C$ is a vector space over $\mathbf{C}$ with basis $x^k y^{-1} dx$ for $k = 0, \ldots, g-1$ (see e.g. [41, Example A.6.2.1]). Note that the morphism $\iota(\zeta)$ acts on this basis as $\iota(\zeta) x^k y^{-1} dx = \zeta^{k+1} x^k y^{-1} dx$, i.e., as the diagonal matrix $M$ with entries in $\Phi(\zeta)$ for the CM-type $\Phi = \{\zeta \mapsto \zeta^l : l = 1, \ldots, g\}$. This basis has a dual basis of $H^0(\omega_C)^*$ and $\zeta$ also acts as $M$ on this dual basis. We find that $(J(C), \iota)$ is of type $\Phi$.

The Jacobian $J(C)$ comes with a natural principal polarization. If we denote by $\cdot$ the intersection pairing on $H_1(C, \mathbf{Z})$ extended $\mathbf{R}$-linearly to $H^0(\omega_C)^*$, then $E : (u, v) \mapsto -u \cdot v$ defines this principal polarization on $J(C)$.

We have now associated to every complex curve a principally polarized abelian variety. Next, we recall that this in fact gives a bijection between the set of curves of genus 2 up to isomorphism and a certain set of principally polarized abelian surfaces up to isomorphism.

**Theorem 6.2** (Torelli)**.** *Two algebraic curves over* $\mathbf{C}$ *are isomorphic if and only if their Jacobians are isomorphic (as polarized abelian varieties).*

*Proof.* This is Theorem 11.1.7 of [4]. □

The product of two polarized abelian varieties $(T_1, E_1)$ and $(T_2, E_2)$ has a natural polarization $(v, w) \mapsto E_1(v_1, w_1) + E_2(v_2, w_2)$ called the *product polarization.*

**Theorem 6.3** (Weil)**.** *Any principally polarized abelian surface over* $\mathbf{C}$ *is either a product of elliptic curves with the product polarization or the Jacobian of a smooth projective curve of genus* 2*.*

*Proof.* This is Satz 2 of [94]. Alternatively, see Corollary 11.8.2 of [4], or see Remark II.7.12 below. □

# 7 The reflex of a CM-type

Let $K$ be a CM-field and let $\Phi$ be a CM-type of $K$ with values in $L'$. Let $L \supset K$ be the normal closure of $K$. Then by making $L'$ smaller, we can assume $L' \cong L$.

The *reflex* $(K^{\mathrm{r}}, \Phi^{\mathrm{r}})$ of $(K, \Phi)$ is defined as follows. Let $\Phi_L$ be the CM-type of $L$ with values in $L'$ induced by $\Phi$. Note that $\Phi_L$ is a set of isomorphisms $L \to L'$, so we can take its set $\Phi_L^{-1}$ of inverses, which is a set of isomorphisms $L' \to L$.

It follows easily from Lemma 2.2(c) that $\Phi_L^{-1}$ is a CM-type of $L'$ with values in $L$ (see also [64, Example 1.28] or [52, Thm. I.5.1(ii)]). By Lemma 3.5, there is a unique primitive pair $(K^{\mathrm{r}}, \Phi^{\mathrm{r}})$ that induces $(L', \Phi_L^{-1})$. We show in Lemma 7.3 that this definition of $K^{\mathrm{r}}$ is equivalent to the one given in Section 4.

**Definition 7.1.** The pair $(K^{\mathrm{r}}, \Phi^{\mathrm{r}})$ is called the *reflex* of $(K, \Phi)$, the field $K^{\mathrm{r}}$ is called the *reflex field* of $(K, \Phi)$, and the CM-type $\Phi^{\mathrm{r}}$ is called the *reflex type* of $(K, \Phi)$.

**Lemma 7.2.** *The CM-type $\Phi^{\mathrm{r}}$ is a primitive CM-type of $K^{\mathrm{r}}$. If we denote the reflex of $(K^{\mathrm{r}}, \Phi^{\mathrm{r}})$ by $(K^{\mathrm{rr}}, \Phi^{\mathrm{rr}})$, then $K^{\mathrm{rr}}$ is a subfield of $K$ and $\Phi$ is induced by $\Phi^{\mathrm{rr}}$. If $\Phi$ is primitive, then we have $K^{\mathrm{rr}} = K$ and $\Phi^{\mathrm{rr}} = \Phi$.*

*Proof.* Primitivity and the facts that $K^{\mathrm{rr}} \subset K$ holds and $\Phi^{\mathrm{rr}}$ induces $\Phi$ follow directly from our definition. If $\Phi$ is primitive, then this implies $K^{\mathrm{rr}} = K$ and hence $\Phi^{\mathrm{rr}} = \Phi$. See also [78, paragraph above Prop. 29 in §8.3] or [52, Thm. 5.2]. □

The following result shows that the definition of the reflex field in the current section coincides with the one given in Section 4.

**Lemma 7.3.** *The reflex field $K^{\mathrm{r}}$ satisfies*

$$\mathrm{Gal}(L'/K^{\mathrm{r}}) = \{\sigma \in \mathrm{Gal}(L'/\mathbf{Q}) \mid \sigma\Phi = \Phi\}.$$

*Proof.* This is exactly what follows from equation (3.6) and the definition of $K^{\mathrm{r}}$. See also [64, Example 1.28]. □

**Example 7.4** (Example 8.4(1) of [78])**.** If a CM-field $K$ is abelian over $\mathbf{Q}$ and $\Phi$ is a primitive CM-type, then $K^{\mathrm{r}}$ is isomorphic to $K$. Indeed, if we choose an isomorphism $L \to L'$, then commutativity of the Galois group implies that the groups of Lemmas 3.5 and 7.3 coincide.

**Example 7.5** (Example 8.4(2)(C) of [78])**.** Let $K$ be a non-Galois quartic CM-field. By Lemma 3.4, the normal closure $L$ of $K$ has Galois group $D_4 = \langle r, s\rangle$ with $r^4 = s^2 = (rs)^2 = e$. The complex conjugation automorphism $\bar{\cdot}$ equals $r^2$ in this notation. Without loss of generality, we have that $s$ is the generator of $\mathrm{Gal}(L/K)$.

For simplicity, we consider CM-types with values in $L$. In other words, we identify $L'$ with $L$ via an isomorphism. The CM-types up to equivalence are $\Phi = \{\mathrm{id}, r_{|K}\}$ and $\Phi' = \{\mathrm{id}, r^3_{|K}\}$ (see Lemma 3.4).

The CM-type induced by $\Phi$ on $L$ is $\Phi\langle s\rangle = \{e, r, s, rs\}$, which has inverse $\{e, r^3, s, rs\} = \{e, r^3\}\langle rs\rangle$. In particular, the reflex field $K^{\mathrm{r}}$ of $\Phi$ is the fixed field of $\langle rs\rangle$, which is a quartic CM-field that is not isomorphic to $K$. The reflex type of $\Phi$ is the CM-type $\{\mathrm{id}, r^3_{|K^{\mathrm{r}}}\}$ of $K^{\mathrm{r}}$.

Similarly, the reflex field of $\Phi'$ is the fixed field of $\langle r^3 s\rangle$, which is conjugate, but not equal, to $K^{\mathrm{r}}$.

**Lemma 7.6.** *The reflex field $K^{\mathrm{r}}$ is generated over $\mathbf{Q}$ by the elements of $L'$ of the form $\sum_{\phi\in\Phi} \phi(x)$ for $x \in K$.*

*Proof.* This is [78, Prop. 28 in §8.3]. □

**Example 7.7.** Let $K$ be a non-Galois quartic CM-field, and write

$$K = \mathbf{Q}(\alpha) \quad \text{with} \quad \alpha = \sqrt{-a + b\sqrt{d}}.$$

Let $\Phi$ be a CM-type of $K$ with values in a field $L'$, and let $\alpha_1, \alpha_2 \in L'$ be the images of $\alpha$ under the embeddings of $\Phi$. We have

$$\alpha_1 = \sqrt{-a + b\sqrt{d}} \quad \text{and} \quad \alpha_2 = \sqrt{-a - b\sqrt{d}}$$

for some choice of the square roots.

By Lemma 7.6, we have $\beta_1 = \alpha_1 + \alpha_2 \in K^{\mathrm{r}}$, where

$$\beta_1^2 = \alpha_1^2 + \alpha_2^2 + 2\alpha_1\alpha_2 = -2a + 2w \tag{7.8}$$

for some square root $w \in L'$ of $a^2 - b^2 d$.

We claim that $\beta_1 = \sqrt{-2a + 2w}$ generates $K^{\mathrm{r}}$ over $\mathbf{Q}$. Indeed, the field $\mathbf{Q}(\beta_1)$ contains $w = \alpha_1\alpha_2$, which is not rational because $K$ is not normal over $\mathbf{Q}$, and which is real because $\alpha_1$ and $\alpha_2$ are purely imaginary. We also find $\beta_1^2 < 0$ for every embedding into $\mathbf{R}$ by equation (7.8), which shows that $\mathbf{Q}(\beta_1)$ is a quartic CM-field. As $\beta_1$ is contained in $K^{\mathrm{r}}$, which is quartic by Example 7.5, this proves the claim.

Note that the element $w = \alpha_1\alpha_2 \in L'$, and hence the quartic field $K^{\mathrm{r}} = \mathbf{Q}(\beta_1) \subset L'$, are uniquely determined by $\Phi$.

The reflex field of $\Phi'$ is then the conjugate $\mathbf{Q}(\beta_2)$ of $K^{\mathrm{r}}$ with $\beta_2 = \sqrt{-2a-2w}$.

The reflex type $\Phi^{\mathrm{r}}$ of $\Phi$ consists of the two embeddings $K^{\mathrm{r}} \to L$ given by $\beta_1 \mapsto \alpha \pm \alpha' \in L'$, where $\alpha' \in L \setminus K$ is a conjugate of $\alpha$ (see Example 7.5).

# 8 The type norm

**Definition 8.1.** Let $\Phi$ be a CM-type of $K$ with values in $L'$. The *type norm* of $\Phi$ is the map

$$\begin{aligned} N_\Phi : K &\to K^{\mathrm{r}} \qquad \subset L' \\ x &\mapsto \prod_{\phi\in\Phi} \phi(x). \end{aligned}$$

The image of the type norm lies in $K^{\mathrm{r}}$ by Lemma 7.3.

**Example 8.2.** The element $w \in K^{\mathrm{r}}$ of Example 7.7 is the type norm $N_\Phi(\alpha)$ of the element $\alpha \in K$ of that example.

The type norm is multiplicative and hence restricts to a homomorphism of unit groups $K^* \to K^{\mathrm{r}*}$.

For any number field $M$, let $I_M$ denote the group of non-zero fractional ideals of $\mathcal{O}_M$ and let $\mathrm{Cl}_M = K^*\backslash I_M$ be the class group.

**Lemma 8.3.** *The type norm induces homomorphisms*

$$\begin{aligned} N_\Phi : I_K &\to I_{K^{\mathrm{r}}} \\ \mathfrak{a} &\mapsto \mathfrak{a}' \qquad \textit{where} \quad \mathfrak{a}'\mathcal{O}_{L'} = \prod_{\phi\in\Phi} \phi(\mathfrak{a})\mathcal{O}_{L'}, \quad \textit{and} \\ N_\Phi : \mathrm{Cl}_K &\to \mathrm{Cl}_{K^{\mathrm{r}}}. \end{aligned}$$

*Proof.* On the groups of ideals $I_K$, this is [52, Remark on page 63]. See also [78, Prop. 29 in §8.3]. As elements of $K^*$ are mapped to $K^{\mathrm{r}*}$, we find the map on class groups. □

It is easy to see that we have

$$\begin{aligned} N_\Phi(x)\overline{N_\Phi(x)} &= N_{K/\mathbf{Q}}(x) \quad \text{for all } x \in K^*, \text{ and} \\ N_\Phi(\mathfrak{a})\overline{N_\Phi(\mathfrak{a})} &= N_{K/\mathbf{Q}}(\mathfrak{a}) \quad \text{for all } \mathfrak{a} \in I_K, \end{aligned}$$

where $N_{K/\mathbf{Q}}$ is the norm, taking positive values in $\mathbf{Q}^*$ and $\bar{\cdot}$ is complex conjugation on $K^{\mathrm{r}}$ (which doesn't depend on a choice of complex embedding since $K^{\mathrm{r}}$ is a CM-field).

For quartic CM-fields, the type norm of the type norm will be a useful tool.

**Lemma 8.4.** *Let* $\mathfrak{a}$ *be an ideal in a primitive* quartic *CM-field* $K$ *and* $\Phi$ *a CM-type. Then we have*

$$N_{\Phi^{\mathrm{r}}} N_{\Phi}(\mathfrak{a}) = N_{K/\mathbf{Q}}(\mathfrak{a}) \frac{\mathfrak{a}}{\overline{\mathfrak{a}}}.$$

*Proof.* By choosing an isomorphism $L \to L'$, we have without loss of generality $\Phi = \{\mathrm{id}, r_{|K}\}$ with $r \in \mathrm{Gal}(L/\mathbf{Q})$ of order 4. If $K$ is non-Galois, then this is Example 7.5, otherwise it is analogous.

We then have $\Phi^{\mathrm{r}} = \{\mathrm{id}, r^3_{|K^{\mathrm{r}}}\}$, hence

$$N_{\Phi^{\mathrm{r}}} N_{\Phi}(\mathfrak{a})\mathcal{O}_L = (\mathfrak{a})^2 (r\mathfrak{a})(r^3\mathfrak{a})\mathcal{O}_L.$$

As $\{\mathrm{id}, r_{|K}, r^2_{|K}, r^3_{|K}\}$ is the set of all embeddings $K \to L$ and we have $\overline{\mathfrak{a}} = r^2\mathfrak{a}$, the result follows. □

# 9 The main theorem of complex multplication

The main theorem of complex multiplication shows how to obtain certain class fields from abelian varieties with complex multiplication. We will now describe which fields they are.

Given a CM-field $F$ with primitive CM-type $\Psi$, let $(K, \Phi)$ be the reflex. Given any ideal $\mathfrak{b} \subset \mathcal{O}_K$, let $b\mathbf{Z} = \mathfrak{b} \cap \mathbf{Z}$ and let $I_F(b)$ be the group of invertible fractional ideals of $F$ that are coprime to $b$. Let

$$H_{F,\Psi}(\mathfrak{b}) = \left\{ \mathfrak{a} \in I_F(b) : \begin{array}{l} \exists \mu \in K^* \text{ such that} \\ N_{\Psi}(\mathfrak{a}) = \mu\mathcal{O}_K, \\ \mu\overline{\mu} = N_{F/\mathbf{Q}}(\mathfrak{a}), \\ \mu \equiv 1 \pmod{^*\mathfrak{b}} \end{array} \right\}$$
$$\supset P_F(b) = \{x\mathcal{O}_F : x \in F^*, \quad x \equiv 1 \pmod{^*b}\},$$

where the inclusion '$\supset$' follows by taking $\mu = N_{\Psi}(x)$. Then the class field $CM_{F,\Psi}(\mathfrak{b})$ corresponding to the ideal group

$$I_F(b)/H_{F,\Psi}(\mathfrak{b})$$

can be obtained using complex multiplication. For the case $b = 1$, we omit $(b)$ from the notation.

Here are the details of how to obtain this field. Embed $F$ into $\mathbf{C}$ and let $A$ be a polarized abelian variety over $\mathbf{C}$ with CM by $\mathcal{O}_K$ via $\iota$

of type $\Phi$. Let $t \in A(\overline{k})$ be a point with annihilator $\mathfrak{b}$. (Such a point exists by [78, Prop. 21 in §7.5].)

To the pair $(A, t)$, one can assign a point $j = j(A, t)$ in a an algebraic *moduli space*. This point is defined over $\overline{\mathbf{Q}} \subset \mathbf{C}$ and can be expressed explicitly in terms of *theta functions*, which are modular forms for a *Siegel modular group*. We do this explicitly for the case $b = 1$ in the next two chapters. See especially Section II.7 and Theorem III.5.2.

**Theorem 9.1.** *With the notation above, we have*

$$\mathrm{CM}_{F,\Psi}(\mathfrak{b}) = F(j(A, t)) \subset \overline{k}.$$

*The action of the Galois group $I_F(b)/H_{F,\Psi}(\mathfrak{b})$ is as follows. Let $(\Phi, \mathfrak{a}, \xi)$ be a triple as in Section 5.2, and write $t = \Phi(x)$ with $x \in K/\mathfrak{a}$. Use the notation $j(\Phi, \mathfrak{a}, \xi, x) = j((A(\Phi, \mathfrak{a}, \xi), \Phi(x)))$. Then for any $[\mathfrak{c}] \in I_F(b)/H_{F,\Psi}(\mathfrak{b})$ with $\mathfrak{c}^{-1} \subset \mathcal{O}_F$, we have*

$$[\mathfrak{c}]j(\Phi, \mathfrak{a}, \xi, x) = j\left(\Phi, N_\Psi(\mathfrak{c})^{-1}\mathfrak{a}, N_{F/\mathbf{Q}}(\mathfrak{c})\xi, (x \bmod N_\Psi(\mathfrak{c})^{-1}\mathfrak{a})\right).$$

*Proof.* If $\Psi$ is a primitive CM-type of $F$, then this result is Main Theorems 1 and 2 in Sections 15.3 and 16.3 of Shimura and Taniyama [78]. The Galois action is given in the proof of those results. See also [52, Thm. 3.6.1] or [64, Thm. 9.17]. □

We can also look at the action of complex conjugation. Then the result (for $b = 1$) is the following.

**Lemma 9.2** ([52, Prop. 3.5.5])**.** *We have* $\overline{A(\Phi, \mathfrak{a}, \xi)} \cong A(\Phi, \overline{\mathfrak{a}}, \xi)$.

**Corollary 9.3.** Suppose $F$ (and hence $K$) is a primitive quartic CM-field. If $A/\mathbf{C}$ is a principally polarized abelian surface with CM by $\mathcal{O}_K$ of type $\Phi$, then every $\mathrm{Gal}(\mathrm{CM}_{F,\Psi}/F_0)$-conjugate of $j(A)$ is also a $\mathrm{Gal}(\mathrm{CM}_{F,\Psi}/F)$-conjugate.

Moreover, the field $F_0(j(A))$ does not contain $F$.

*Proof.* Write $A$ as $A(\Phi, \mathfrak{a}, \xi)$ with $\mathfrak{a}^{-1} \subset \mathcal{O}_K$ and take $\mathfrak{c} = N_\Phi(\mathfrak{a})$.

Theorem 9.1 states

$$[\mathfrak{c}]j(\Phi, \mathfrak{a}, \xi) = j(\Phi, N_\Psi(\mathfrak{c})^{-1}\mathfrak{a}, N_{K/\mathbf{Q}}(\mathfrak{c})\xi),$$

which by Lemma 8.4 is

$$j(\Phi, N_{K/\mathbf{Q}}(\mathfrak{a})^{-1}\overline{\mathfrak{a}}, N_{K/\mathbf{Q}}(\mathfrak{a})^{-2}\xi) = j(\Phi, \overline{\mathfrak{a}}, \xi).$$

By Lemma 9.2, this is exactly the complex conjugate of $j(A)$, so complex conjugation acts on $j(A)$ as $[\mathfrak{c}] \in \mathrm{Gal}(\mathrm{CM}_{F,\Psi}/F)$.

Note that the set $\{\mathrm{id}, \bar{\cdot}\}$ is a complete set of representatives for the quotient group $\mathrm{Gal}(\mathrm{CM}_{F,\Psi}/F_0)/\mathrm{Gal}(\mathrm{CM}_{F,\Psi}/F)$.

The length of the $\mathrm{Gal}(\mathrm{CM}_{F,\Psi}/F_0)$-orbit of $j(A)$ is the degree of $F_0(j(A))/F_0$, and the same holds with $F_0$ everywhere replaced by $F$. We find $\deg F_0(j(A))/F_0 = \deg F(j(A))/F = \frac{1}{2}\deg F(j(A))/F_0$, hence $F(j(A))$ is not equal to $F_0(j(A))$, which proves that $F_0(J(A))$ does not contain $F$. □

# 10 The class fields of quartic CM-fields

Next, let us see which class fields we can obtain using complex multiplication. Suppose first that $F$ is imaginary quadratic. Then $\Psi$ is an isomorphism $F \to K$ and $\Phi$ is its inverse, so we identify $F$ and $K$ via these maps. We find that in that case

$$H_{F,\Psi}(\mathfrak{b}) = P_F(\mathfrak{b}) := \{x\mathcal{O}_F : x \in F^*, x \equiv 1 \pmod^*\mathfrak{b}\}$$

holds, so $\mathrm{CM}_{F,\Psi}(\mathfrak{b})$ is the *ray class field* of $F = K$ of modulus $\mathfrak{b}$. In particular, every finite abelian extension of $F$ is a subfield of some $H_{F,\Psi}(\mathfrak{b})$, so CM theory can construct all such fields.

If $F$ is a CM-field of degree $> 2$, then CM theory by itself is insufficient for constructing all class fields. However, Shimura [76] describes how to obtain all abelian extensions of $F$ using a combination of

(1) CM theory,

(2) the ray class fields of the maximal totally real subfield $F_0 \subset F$, and

(3) quadratic Kummer extensions of the fields that one obtains with (1) and (2).

**Remark 10.1.** For imaginary quadratic $F$, we have $F_0 = \mathbf{Q}$, and the class fields of $\mathbf{Q}$ are contained in the cyclotomic fields by the Kronecker-Weber Theorem 1.1. These cyclotomic fields can be obtained from the torsion points via the Weil pairing, which explains why we do not need to separately consider the class fields of $F_0$ for imaginary quadratic fields $F$.

**Theorem 10.2** (Theorem 1 of Shimura [76])**.** *Let $F$ be a CM-field, $\Psi$ a CM-type of $F$, and $\psi \in \Psi$ an element such that the reflex field of $(F,\Psi)$ is contained in $\psi(F)$. Let $\Psi'$ be obtained from $\Psi$ by replacing $\psi$ by its complex conjugate $\overline{\psi}$. Let $b$ be a positive integer and $H_F(b)$ (resp.*

*$H_{F_0}(b)$) be the ray class field of modulus $b$ of $F$ (resp. $F_0$). Then the abelian extension*

$$H_F(b) \supset H_{F_0}(b) \cdot \mathrm{CM}_{F,\Psi}(b) \cdot \mathrm{CM}_{F,\Psi'}(b)$$

*has exponent* 1 *or* 2. □

Note that Kummer extensions of exponent 2 can be constructed without adjoining additional roots of unity. So far so good. However, Theorem 10.2 doesn't apply to non-Galois quartic CM-fields, because they have a reflex field that is quartic and not isomorphic to $F$.

Shimura then fixes this by applying Theorem 10.2 to a CM-type $\Psi'$ of an extension $E$ of $F$ instead of to $F$ itself (see [76, Prop. 8 and Thm. 4]). In the quartic case, the field $E$ is the normal closure of $F$ and $\Psi'$ is primitive, hence the reflex field of $\Psi'$ is isomorphic to $L$, which has degree 8. This implies that Shimura's construction for non-Galois quartic CM-fields requires simple abelian varieties of dimension 4 instead of only abelian surfaces!

We can however replace Theorem 10.2 by the following simpler result that does apply to all primitive quartic CM-fields.

**Theorem 10.3.** *Let $F$ be a primitive quartic CM-field and $\Psi$ a primitive CM-type of $F$. Let $b$ be a positive integer and $H_F(b)$ (resp. $H_{F_0}(b)$) be the ray class field of modulus $b$ of $F$ (resp. $F_0$). Then the abelian extension*

$$H_F(b) \supset H_{F_0}(b) \cdot \mathrm{CM}_{F,\Psi}(b)$$

*has exponent* 1 *or* 2.

*Proof.* First recall that the composite $H_{F_0}(b) \cdot F$ is the class field of $F$ corresponding to $I_F(b)/H_0(b)$, where

$$H_0(b) = \{\mathfrak{a} \in I_F(b) : \mathfrak{a}\overline{\mathfrak{a}} = v\mathcal{O}_F, v \in F_0^*, v \equiv 1 \pmod^* b\}.$$

As $H_F(b)$ has Galois group $I_F(b)/P_F(b)$, it has exponent 1 or 2 over the class field corresponding to the group $I_F(b)/B$ with

$$B = \{\mathfrak{a} \in I_F(b) : \mathfrak{a}^2 \in P_F(b)\}.$$

Therefore, it suffices to prove $H_0(b) \cap H_{F,\Psi}(b) \subset B$.

Let $\mathfrak{a} \in H_0(b) \cap H_{F,\Psi}(b)$ be any element. Let $v$ and $\mu$ be as in the definitions of $H_0(b)$ and $H_{F,\Psi}(b)$. Then we have by Lemma 8.4,

$$\begin{aligned}\mathfrak{a}^2 &= N_{\Psi^r} N_\Psi(\mathfrak{a}) \frac{\mathfrak{a}\overline{\mathfrak{a}}}{N_{F/\mathbf{Q}}(\mathfrak{a})} \\ &= N_{\Psi^r}(\mu) \frac{v}{N_{F_0/\mathbf{Q}}(v)} \mathcal{O}_F.\end{aligned}$$

As the generators $\mu$ and $v$ are 1 $(\mathrm{mod}^* b)$, so is the generator of $\mathfrak{a}^2$ that we have just given. □

**Example 10.4.** The non-Galois quartic CM-field

$$F = \mathbf{Q}(\sqrt{-27 + 4\sqrt{13}})$$

has class number 7 and a real quadratic subfield $F_0 = \mathbf{Q}(\sqrt{13})$ of class number 1. We conclude from Theorem 10.3 that $\mathrm{CM}_{F,\Psi}$ equals the Hilbert class field of $F$, because 7 is odd and we have $H_{F_0} = F_0 \subset F$. We will compute a defining polynomial of $\mathrm{CM}_{F,\Psi}$ in Example III.3.2.

A *non*-primitive quartic CM-field $F$ has two imaginary quadratic subfields $F_1$ and $F_2$ by Lemma 3.4. The ray class fields of these fields can be obtained by complex multiplication of elliptic curves. The ray class fields of $F$ itself can be obtained from the ray class fields of $F_0$, $F_1$, and $F_2$ using the following general result.

**Theorem 10.5.** *Let $F/N$ be a Galois extension of number fields with Galois group $V_4$, and let $F_0$, $F_1$, $F_2$ be the intermediate fields. Let $b$ be a positive integer and let $H_F(b)$ (resp. $H_{F_j}(b)$) be the ray class field of modulus $b$ of $F$ (resp. $F_j$). Then the abelian extension*

$$H_F(b) \supset H_{F_0}(b) \cdot H_{F_1}(b) \cdot H_{F_2}(b)$$

*has exponent* 1 *or* 2.

*Proof.* As in the proof of Theorem 10.3, it suffices to show that the intersection of the three groups

$$H_i(b) = \{\mathfrak{a} \in I_F(b) : \mathfrak{a}(a_i(\mathfrak{a})) = v\mathcal{O}_F, v \in F_i^*, v \equiv 1 \ (\mathrm{mod}^* b)\}$$

is contained in the group

$$B = \{\mathfrak{a} \in I_F(b) : \mathfrak{a}^2 \in P_F(b)\}.$$

Let $\mathfrak{a}$ be any element of this intersection, and take $v_i$ as in the definition of $H_i(b)$. Let $a_i \in \mathrm{Gal}(F/F_i)$ be a generator, so we have $v_i\mathcal{O}_F = \mathfrak{a}(a_i\mathfrak{a})$ and $\mathrm{Gal}(F/N) = \{\mathrm{id}, a_0, a_1, a_2\} \cong C_2 \times C_2$. We get

$$\mathfrak{a}^2 = v_1 v_2 a_1(v_0)^{-1}\mathcal{O}_F,$$

and $v_1 v_2 a_1(v_0)^{-1} \equiv 1 \ (\mathrm{mod}^* b)$. □

Chapter II

# Computing Igusa class polynomials

Abstract. *We give an algorithm that computes the genus-two class polynomials of a primitive quartic CM-field $K$, and we give a running time bound and a proof of correctness of this algorithm. This is the first proof of correctness and the first running time bound of any algorithm that computes these polynomials.*

## 1 Introduction

The *Hilbert class polynomial* $H_K \in \mathbf{Z}[X]$ of an imaginary quadratic number field $K$ has as roots the $j$-invariants of complex elliptic curves having complex multiplication (CM) by the ring of integers of $K$. These roots generate the Hilbert class field of $K$, and Weber [93] computed $H_K$ for many small $K$. The CM method uses the reduction of $H_K$ modulo large primes to construct elliptic curves over $\mathbf{F}_p$ with a prescribed number of points, for example for cryptography. The bit size of $H_K$ grows exponentially with the bit size of $K$: it grows like the discriminant $\Delta$ of $K$, and so does the running time of the algorithms that compute it ([22, 2]).

If we go from elliptic curves (genus 1) to genus-2 curves, we get the *Igusa class polynomials* $H_{K,n} \in \mathbf{Q}[X]$ $(n = 1, 2, 3)$ of a *quartic CM-field* $K$. Their roots are the Igusa invariants of all complex genus-

2 curves having CM by the ring of integers of $K$. As in the case of genus 1, these roots generate class fields and the reduction of Igusa class polynomials modulo large primes $p$ yields cryptographically interesting curves of genus 2. Computing Igusa class polynomials is considerably more complicated than computing Hilbert class polynomials, in part because of their denominators. Recently, various algorithms have been developed: a complex analytic method by Spallek [79] and van Wamelen [88], a $p$-adic method by Gaudry, Houtmann, Kohel, Ritzenthaler, and Weng [31, 32] and Carls, Kohel, and Lubicz [13, 14], and a Chinese remainder method by Eisenträger and Lauter [21], but no running time or precision bounds were available.

This chapter describes a complete and correct algorithm that computes Igusa class polynomials $H_{K,n} \in \mathbf{Q}[X]$ of *quartic CM-fields* $K = \mathbf{Q}(\sqrt{\Delta_0}, \sqrt{-a+b\sqrt{\Delta_0}})$, where $\Delta_0$ is a real quadratic fundamental discriminant and $a, b \in \mathbf{Z}$ are such that $-a+b\sqrt{\Delta_0}$ is totally negative. Our algorithm is based on the complex analytic method of Spallek and van Wamelen. The discriminant $\Delta$ of $K$ is of the form $\Delta = \Delta_1\Delta_0^2$ for a positive integer $\Delta_1$. We may and will assume $0 < a < \Delta$, as Lemma 9.9 below shows that each quartic CM-field has such a representation. We disregard the degenerate case of *non-primitive* quartic CM-fields, i.e., those that can be given with $b = 0$, as abelian varieties with CM by non-primitive quartic CM-fields are isogenous to products of CM elliptic curves, which can be obtained already using Hilbert class polynomials. We give the following running time bound for our algorithm, where we use $\widetilde{O}(g)$ to mean "at most $g$ times a polynomial in $\log g$".

**Main Theorem.** *Algorithm 11.1 computes $H_{K,n}$ ($n = 1, 2, 3$) for any primitive quartic CM-field $K$. It has a running time of $\widetilde{O}(\Delta_1^{7/2}\Delta_0^{11/2})$ and the bit size of the output is $\widetilde{O}(\Delta_1^2\Delta_0^3)$.*

An essential part of the proof is the denominator bound, as provided by Goren and Lauter [35, 36].

We do not claim that the bound on our running time is optimal, but an exponential running time is unavoidable, because the degree of the Igusa class polynomials (as with Hilbert class polynomials) is already bounded from below by a power of the discriminant.

## Overview

Section 2 provides a precise definition of the Igusa class polynomials that we will work with, and mentions other definitions occurring in

the literature. Our main theorem is valid for all types of Igusa class polynomials.

Instead of enumerating curves, it is easier to enumerate their Jacobians, which are principally polarized abelian varieties. Van Wamelen [88] gave a method for enumerating all isomorphism classes of principally polarized abelian varieties with CM by a given order. We give an improvement of his results in Section 3.

Section 4 shows how principally polarized abelian varieties give rise to points in the *Siegel upper half space* $\mathcal{H}_2$. These points are matrices known as *period matrices*. Two period matrices correspond to isomorphic principally polarized abelian varieties if and only if they are in the same orbit under the action of the *symplectic group* $\mathrm{Sp}_4(\mathbf{Z})$.

In Section 5, we analyze a reduction algorithm that replaces period matrices by $\mathrm{Sp}_4(\mathbf{Z})$-equivalent period matrices in a *fundamental domain* $\mathcal{F}_2 \subset \mathcal{H}_2$. In Section 6, we give an upper bound on the entries of the reduced period matrices computed in Section 5.

Absolute Igusa invariants can be computed from period matrices by means of *theta constants*. Section 7 introduces theta constants and gives formulas that express Igusa invariants in terms of theta constants. The formulas that we give are much simpler than those that appear in [79, 97] or the textbook [27], reducing the formulas from more than a full page to only a few lines. We then give bounds on the absolute values of theta constants and Igusa invariants in terms of the entries of the reduced period matrices computed in Section 5. We finish Section 7 by showing how to evaluate the theta constants, and hence the absolute Igusa invariants, to a given precision.

Section 8 bounds the degree of Igusa class polynomials and Section 9 gives the bounds of Goren and Lauter [35, 36] on the denominators. Section 10 shows how to reconstruct a rational polynomial from its complex roots, and the precision needed for that in terms of an upper bound on the denominator of the polynomial and the absolute values of the zeroes.

Finally, Section 11 puts all the results together into a single algorithm and a proof of the main theorem.

# 2 Igusa class polynomials

The *Hilbert class polynomial* of an imaginary quadratic number field $K$ is the polynomial of which the roots in $\mathbf{C}$ are the *$j$-invariants* of the elliptic curves over $\mathbf{C}$ with complex multiplication by the ring of integers $\mathcal{O}_K$ of $K$. For a genus-2 curve, one needs three invariants, the *absolute*

*Igusa invariants* $i_1, i_2, i_3$, instead of one, to fix its isomorphism class.

## 2.1 Igusa invariants

Let $k$ be a field of characteristic different from 2. Any curve of genus 2 over $k$, i.e., a projective, geometrically irreducible algebraic curve over $k$ of which the genus is 2, has an affine model of the form $y^2 = f(x)$, where $f \in k[x]$ is a separable polynomial of degree 6. Let $\alpha_1, \ldots, \alpha_6$ be the six distinct roots of $f$ in $\overline{k}$, and let $a_6$ be the leading coefficient. For any permutation $\sigma \in S_6$, let $(ij)$ denote the difference $(\alpha_{\sigma(i)} - \alpha_{\sigma(j)})$. We can then define the *homogeneous Igusa-Clebsch invariants* in compact notation that we explain below, as

$$\begin{aligned}
I_2 &= a_6^2 \sum_{15} (12)^2(34)^2(56)^2, \\
I_4 &= a_6^4 \sum_{10} (12)^2(23)^2(31)^2(45)^2(56)^2(64)^2, \\
I_6 &= a_6^6 \sum_{60} (12)^2(23)^2(31)^2(45)^2(56)^2(64)^2(14)^2(25)^2(36)^2, \\
I_{10} &= a_6^{10} \prod_{i<j} (\alpha_i - \alpha_j)^2,
\end{aligned}$$

The sum is taken over all distinct expressions (in the roots of $f$) that are obtained when $\sigma$ ranges over $S_6$. The subscript indicates the number of expressions encountered. More precisely, there are 15 ways of partitioning the six roots of $f$ into three subsets of two. Each yields a triple $f_1$, $f_2$, $f_3$ of monic quadratic polynomials over $\overline{k}$, and the summand in $I_2$ is the product of their discriminants. Similarly, for $I_4$ there are 10 ways of partitioning the six roots of $f$ into two subsets of three, and each yields a summand that is the product of two cubic discriminants. For each of the 10 ways of partitioning the six roots of $f$ into two subsets of three, there are 6 ways of giving a bijection between those two subsets, and each gives a summand for $I_6$. Finally, $I_{10}$ is simply the discriminant of $f$, which is non-zero as $f$ is separable. The invariants $I_2, I_4, I_6, I_{10}$ were introduced by Igusa [45], who denoted them by $A, B, C, D$ and based them on invariants of Clebsch [15].

By the symmetry in the definition, each of the homogeneous invariants is actually a polynomial in the coefficients of $f$, hence an element of $k$. Actually, we will use another homogeneous invariant given by $I_6' = \frac{1}{2}(I_2 I_4 - 3I_6)$, which is better than $I_6$ as we will see in Section 7.

We define the *absolute Igusa invariants* by

$$i_1 = \frac{I_4 I_6'}{I_{10}}, \quad i_2 = \frac{I_2 I_4^2}{I_{10}}, \quad i_3 = \frac{I_4^5}{I_{10}^2}.$$

The values of the absolute Igusa invariants of a curve $C$ depend only on the $\overline{k}$-isomorphism class of the curve $C$. For any triple $(i_1^0, i_2^0, i_3^0)$, if 3 and $i_3^0$ are non-zero in $k$, then there exists a curve $C$ of genus 2 (unique up to isomorphism) over $\overline{k}$ with $i_n(C) = i_n^0$ $(n = 1, 2, 3)$, and this curve can be constructed using an algorithm of Mestre [61]. We deal with the case $i_3^0 = 0$ in Section III.5.

**Definition 2.1.** Let $K$ be a primitive quartic CM-field. The *Igusa class polynomials* of $K$ are the three polynomials

$$H_{K,n} = \prod_C (X - i_n(C)) \quad \in \mathbf{Q}[X] \quad (n \in \{1, 2, 3\}),$$

where the product ranges over the isomorphism classes of algebraic genus-2 curves over $\mathbf{C}$ of which the Jacobian has complex multiplication by $\mathcal{O}_K$.

For the definitions of the Jacobian and complex multiplication, see Chapter I. We will see in Section 3 that the product in the definition is indeed finite. The polynomial is rational, because any conjugate of a CM curve has CM by the same order.

## 2.2 Alternative definitions

In the literature, one finds various sets of absolute Igusa invariants [12, 35, 50, 45, 61, 98]. Most notably, Igusa defined homogeneous invariants $J_{2n}$ $(n = 1, \ldots, 5)$ in terms of a general hyperelliptic equation and used them to define absolute invariants that have good reduction behaviour at all primes, including 2 and 3.

A triple of invariants that seems standard (up to the powers of 2) in computations [28, 79, 88, 97] is Spallek's $j_1 = 2^{-3} I_2^5 I_{10}^{-1}$, $j_2 = 2 I_2^3 I_4 I_{10}^{-1}$, $j_3 = 2^3 I_2^2 I_6 I_{10}^{-1}$. However, our choice of absolute invariants $i_1$, $i_2$, $i_3$ yields Igusa class polynomials of much smaller height, both experimentally (see Appendix 3.1) and in terms of the proven bounds of Corollary 7.11 and Theorem 9.1. See also Remarks 7.6 and 9.3.

If the base field $k$ has characteristic 0, then Igusa's and Spallek's absolute invariants, as well as most of the other invariants in the literature, lie in the $\mathbf{Q}$-algebra $A$ of homogeneous elements of degree 0 of $\mathbf{Q}[I_2, I_4, I_6, I_{10}^{-1}]$. Our main theorem remains true if $(i_1, i_2, i_3)$ in the definition of the Igusa class polynomials is replaced by any finite list of elements of $A$.

**Interpolation formulas**

If we take one root of each of the Igusa class polynomials, then we get a triple of invariants and thus (if $i_3 \neq 0$) an isomorphism class of curve of genus 2, which doens't necessarily have CM. That way, the three Igusa class polynomials describe $d^3$ triples of invariants, where $d$ is the degree of the polynomials. The $d$ triples corresponding to curves with CM by $\mathcal{O}_K$ are among them, but the Igusa class polynomials give no means of telling which they are.

To solve this problem, (and thus greatly reduce the number of curves to be checked during explicit CM constructions), we use the following modified Lagrange interpolation:

$$\widehat{H}_{K,n} = \sum_C \left( i_n(C) \prod_{C' \neq C} (X - i_1(C')) \right) \quad \in \mathbf{Q}[X], \quad (n \in \{2,3\}).$$

If $H_{K,1}$ has no roots of multiplicity greater than 1, then the triples of invariants corresponding to curves with CM by $\mathcal{O}_K$ are exactly the triples $(i_1, i_2, i_3)$ such that

$$H_{K,1}(i_1) = 0, \quad i_n = \frac{\widehat{H}_{K,n}(i_1)}{H'_{K,1}(i_1)} \quad (n \in \{2,3\}).$$

Our main theorem is also valid if we replace $H_{K,2}$ and $H_{K,3}$ by $\widehat{H}_{K,2}$ and $\widehat{H}_{K,3}$.

If $H_{K,1}$ has only double roots, then these interpolation formulas are useless. In practice, this never happens, and we deal with the theoretical possibility that it does happen in Section III.5.

This way of representing algebraic numbers like our $i_2$, $i_3$ in terms of others appears in Hecke [40, Hilfssatz a in §36], and is sometimes called *Hecke representation* [38, 23]. The idea to use this modified Lagrange interpolation in the definition of Igusa class polynomials is due to Gaudry, Houtmann, Kohel, Ritzenthaler, and Weng [32], who give a heuristic argument that the height of the polynomials $\widehat{H}_{K,n}$ is smaller than the height of the usual Lagrange interpolation.

# 3 Abelian varieties with CM

Instead of enumerating CM curves, we enumerate their *Jacobians*, which are principally polarized abelian varieties. In the current section, we give an algorithm that computes a representative of every isomorphism class

of complex principally polarized abelian varieties with CM by the ring of integers $\mathcal{O}_K$ of a primitive quartic CM-field $K$.

Section 3.1 gives the general algorithm, for CM-fields of arbitrary degree, Section 3.2 specializes to the case of quartic CM-fields, and Section 3.3 gives details on how ideals should be represented and computed.

## 3.1 The general algorithm

---

**Algorithm 3.1.**
**Input:** A CM-field $K$ with maximal totally real subfield $K_0$ such that $K$ does not contain a strict CM-subfield.
**Output:** A complete set of representatives for the equivalence classes of principally polarized abelian varieties over $\mathbf{C}$ with CM by $\mathcal{O}_K$, each given by a triple $(\Phi, \mathfrak{a}, \xi)$ as in Theorem I.5.2.

---

1. Let $T$ be a complete set of representatives of the equivalence classes of CM-types of $K$ with values in $\mathbf{C}$.

2. Let $U$ be a complete set of representatives of the quotient

$$\mathcal{O}_{K_0}^*/N_{K/K_0}(\mathcal{O}_K^*).$$

3. Let $I$ be a complete set of representatives of the ideal class group of $K$.

4. Take those $\mathfrak{a}$ in $I$ such that $(\mathfrak{a}\overline{\mathfrak{a}}\mathcal{D}_{K/\mathbf{Q}})^{-1}$ is principal and generated by an element $\xi \in K$ such that $\xi^2$ is totally negative in $K_0$. For each such $\mathfrak{a}$, choose such an element $\xi \in K$.

5. For every pair $(\mathfrak{a}, \xi)$ as in step 4 and every unit $u \in U$, take the CM-type $\Phi$ consisting of those embeddings of $K$ into $\mathbf{C}$ that map $u\xi$ to the positive imaginary axis.

6. Return those triples $(\Phi, \mathfrak{a}, u\xi)$ of step 5 for which $\Phi$ is in $T$.

---

*Proof.* By Theorem I.5.2.1, the output consists only of principally polarized abelian varieties with CM by $\mathcal{O}_K$. Conversely, by Theorem I.5.2.2, every principally polarized abelian variety $A$ with CM by $\mathcal{O}_K$ is isomorphic to $A(\Phi, \mathfrak{a}, \xi)$ for some triple $(\Phi, \mathfrak{a}, \xi)$, where $\Phi$ is the CM-type of $A$.

By Lemmas I.5.4 and I.5.6, the CM-type $\Phi$ is unique exactly up to equivalence of CM-types. This uniquely determines $\Phi$ in $T$.

By Theorem I.5.2.4, we can get $\mathfrak{a} \in I$. We get that $A$ is isomorphic to $A(\Phi, \mathfrak{a}, u\xi)$ for some $u \in \mathcal{O}_{K_0}^*$ and a unique triple $(\Phi, \mathfrak{a}, \xi)$ with $\Phi \in T$, $\mathfrak{a}$ in the set of step 4, and $\xi$ as found in step 4. Only the choice of $u \in \mathcal{O}_{K_0}^*$ is left and by Theorem I.5.2.4, the isomorphism class of $A(\Phi, \mathfrak{a}, u\xi)$ depends exactly on the class of $u$ in $\mathcal{O}_{K_0}^*/N_{K/K_0}(\mathcal{O}_K^*)$. □

**Remark 3.2.** Algorithm 3.1 is basically Algorithm 1 of van Wamelen [88] with the difference that we do not have any duplicate abelian varieties.

## 3.2 Quartic CM-fields

We now describe, in the quartic case, the sets $T$ and $U$ of Algorithm 3.1, and the number of isomorphism classes of principally polarized CM abelian surfaces.

By Lemma I.3.4, we can take the set $T$ to consist of a single CM-type if $K$ is cyclic and we can take $T = \{\Phi, \Phi'\}$ if $K$ is non-Galois. The corollary to the following lemma gives the set $U$.

**Lemma 3.3.** *If $K$ is a primitive quartic CM-field, then*

$$\mathcal{O}_K^* = \mu_K \mathcal{O}_{K_0}^*,$$

*where $\mu_K \subset \mathcal{O}_K^*$ is the group of roots of unity, which has order 2 or 10.*

*Proof.* As $K$ has degree 4 and does not contain a primitive third or fourth root of unity, it is either $\mathbf{Q}(\zeta_5)$ or does not contain a root of unity different from $\pm 1$. This proves that $\mu_K$ has order 2 or 10. A direct computation shows that the lemma is true for $K = \mathbf{Q}(\zeta_5)$, so we assume that we have $\mu_K = \{\pm 1\}$.

Let $\epsilon$ (resp. $\epsilon_0$) be a generator of $\mathcal{O}_K^*$ (resp. $\mathcal{O}_{K_0}^*$) modulo torsion. Then without loss of generality, we have $\epsilon_0 = \epsilon^k$ for some positive integer $k$. so either $k = 1$ and we are done, or $k = 2$.

Suppose that we have $k = 2$. As $K = K_0(\sqrt{\epsilon_0})$ is a CM-field, we find that $\epsilon_0$ is totally negative, and hence $\epsilon_0^{-1}$ is the conjugate of $\epsilon_0$. Let $x = \epsilon - \epsilon^{-1} \in K$. Then $x^2 = -2 + \epsilon_0 + \epsilon_0^{-1} = -2 + \mathrm{Tr}(\epsilon_0) \in \mathbf{Z}$ is negative, so $\mathbf{Q}(x) \subset K$ is imaginary quadratic, contradicting primitivity of $K$. □

**Corollary 3.4.** If $K$ is a primitive quartic CM-field, then we have

$$\mathcal{O}_{K_0}^*/N_{K/K_0}(\mathcal{O}_K^*) = \mathcal{O}_{K_0}^*/\mathcal{O}_{K_0}^{*2} = \{\pm 1, \pm c\},$$

where $c$ is the class of the fundamental unit $\epsilon$ of $K_0$.

*Proof.* This follows from Lemma 3.3, because of $N_{K/K_0}(\mu_K) = \{1\}$. □

**Lemma 3.5.** *Let $K$ be a quartic CM-field. If $K$ is cyclic, then there are $h_1$ isomorphism classes of principally polarized abelian surfaces with CM by $\mathcal{O}_K$. If $K$ is non-Galois, then there are $2h_1$ such isomorphism classes.*

*Proof.* Proposition I.5.3 gives the number $h_1 \cdot \#\mathcal{O}_{K_0}^*/N_{K/K_0}(\mathcal{O}_K^*)$, but counts every abelian variety twice if $K$ is non-Galois and four times if $K$ is cyclic Galois (see Lemma I.3.4). Corollary 3.4 shows that we have $\#\mathcal{O}_{K_0}^*/N_{K/K_0}(\mathcal{O}_K^*) = 4$. □

## 3.3 Implementation details

In practice, Algorithm 3.1 takes up only a very small portion of the time needed for Igusa class polynomial computation. The purpose of this section is to show that, for primitive quartic CM-fields, indeed Algorithm 3.1 can be run in time $\widetilde{O}(\Delta)$ and to show that the size of the output for each isomorphism class is small: only polynomial in $\log \Delta$.

It is well known that lists of representatives for the class groups of number fields $K$ of fixed degree can be computed in time $\widetilde{O}(|\Delta|^{\frac{1}{2}})$, where $\Delta$ is the discriminant of $K$. For details, see Schoof [73]. The representatives of the ideal classes that are given in the output are integral ideals of norm below the Minkowski bound, which is $3/(2\pi^2)\,|\Delta|^{1/2}$ for a quartic CM-field.

The algorithms in [73] show that for each $\mathfrak{a}$, we can check in time $\widetilde{O}(|\Delta|^{\frac{1}{2}})$ if $\mathfrak{a}\overline{\mathfrak{a}}\mathcal{D}_{K/\mathbf{Q}}$ is principal and, if so, write down a generator $\xi$. As $\mathcal{O}_K^* = \mu_K \mathcal{O}_{K_0}^*$, it suffices to check, for each of the roots of unity $\zeta$ in $K$, if $\zeta\xi$ is totally imaginary (note that $\mathbf{Q}(\zeta_5)$ is the only primitive quartic CM-field with more than 2 roots of unity). Then the set $T$ and the group $\mathcal{O}_{K_0}^*/N_{K/K_0}(\mathcal{O}_K^*)$ are already given in Section 3.2, where the fundamental unit $\epsilon$ is a by-product of the class group computations. In particular, it takes time at most $\widetilde{O}(|\Delta|)$ to perform all the steps of Algorithm 3.1.

A priori, the bit size of $\xi$ can be as large as the regulator of $K$, but we can easily make it much smaller as follows. We identify $K \otimes \mathbf{R}$ with $\mathbf{C}^2$ via the embeddings $\phi_1, \phi_2$ in the CM-type $\Phi$, and we consider the standard Euclidean norm on $\mathbf{C}^2$. Then we find a short vector

$$b\,|\xi|^{-1/2} = \left(\phi_1(b)\,|\phi_1(\xi)|^{-1/2}, \phi_2(b)\,|\phi_2(\xi)|^{-1/2}\right)$$

in the lattice $\mathcal{O}_K\,|\xi|^{-1/2} \subset \mathbf{C}^2$ using the LLL-algorithm (see [57]) and replace $\mathfrak{a}$ by $b\mathfrak{a}$ and $\xi$ by $(b\overline{b})^{-1}\xi$. By part 4 of Theorem I.5.2, this does

not change the corresponding isomorphism class of principally polarized abelian varieties. This also doesn't change the fact that $\xi^{-1}$ is in $\mathcal{O}_K$ and that $\mathfrak{a}$ is an integral ideal. Finally, we compute an LLL-reduced basis of $\mathfrak{a} \subset \mathcal{O}_K \otimes \mathbf{R} = \mathbf{C}^2$. We get the following result.

**Lemma 3.6.** *If we run Algorithm 3.1 in the way we have just described, then on input of a primitive quartic CM-field $K$, given as*

$$K = \mathbf{Q}(\sqrt{\Delta_0}, \sqrt{-a + b\sqrt{\Delta_0}})$$

*for integers $a, b, \Delta_0$ with $0 < a < \Delta$, it takes time $\widetilde{O}(\Delta)$. For each triple $(\Phi, \mathfrak{a}, \xi)$ in the output, the ideal $\mathfrak{a}$ is given by an LLL-reduced basis, and both $\xi \in K$ and the basis of $\mathfrak{a}$ have bit size $O(\log \Delta)$.*

*Proof.* First, compute the ring of integers $\mathcal{O}_K$ of $K$ using the algorithm of Buchmann and Lenstra [9]. This takes polynomial time plus the time needed to factor the discriminant of the defining polynomial of $K$, which is small enough because of the assumption $0 < a < \Delta$. Then do the class group computations as explained above.

For each triple $(\Phi, \mathfrak{a}, \xi)$, before we apply the LLL-reduction, we can assume that $\mathfrak{a}$ is an integral ideal of norm below the Minkowski bound, hence we have

$$N_{K/\mathbf{Q}}(\xi^{-1}) = N_{K/\mathbf{Q}}(\mathfrak{a})^2 N_{K/\mathbf{Q}}(\mathcal{D}_{K/\mathbf{Q}}) \leq C\Delta^3$$

for some constant $C$.

The covolume of the lattice

$$|\xi|^{-1/2} \mathcal{O}_K \subset \mathcal{O}_K \otimes \mathbf{R} = \mathbf{C}^2$$

is $N_{K/\mathbf{Q}}(\xi^{-1})\Delta^{1/2}$, so we find a vector $b\,|\xi|^{-1/2} \in |\xi|^{-1/2}\,\mathcal{O}_K$ of length at most $C' N_{K/\mathbf{Q}}(\xi^{-1})^{1/8}\Delta^{1/8}$ for some constant $C'$. In particular, $b\bar{b}\xi^{-1}$ has all absolute values below $C'^2 N_{K/\mathbf{Q}}(\xi^{-1})^{1/4}\Delta^{1/4}$. Therefore, $b\bar{b}\xi^{-1}$ has bit size $O(\log \Delta)$ and norm at most $C'^8 N_{K/\mathbf{Q}}(\xi^{-1})\Delta$, so $b$ has norm at most $C'^4\Delta^{1/2}$.

This implies that $b\mathfrak{a}$ has norm at most $C''\Delta$, so an LLL-reduced basis has bit size $O(\log(\mathrm{covol}(b\mathfrak{a}))) = O(\log \Delta)$.

All elements $x \in K$ that we encounter can be given (up to multiplication by units in $\mathcal{O}_{K_0}^*$) with all absolute values below $\sqrt{N_{K/\mathbf{Q}}(a)}\,|\epsilon|$. Therefore, the bit size of the numbers that are input to the LLL-algorithm is $\widetilde{O}(\mathrm{Reg}_K) = \widetilde{O}(\Delta^{1/2})$, hence every execution of the LLL algorithm takes time only $\widetilde{O}(\Delta^{1/2})$ for each ideal class. □

# 4 Symplectic bases

Let $(\mathbf{C}^g/\Lambda, E)$ be a principally polarized abelian variety. For any basis $b_1, \ldots, b_{2g}$ of $\Lambda$, we associate to the form $E$ the matrix $N = (n_{ij})_{ij} \in \mathrm{Mat}_{2g}(\mathbf{Z})$ given by $E(b_i, b_j) = n_{ij}$. We say that $E$ is given with respect to the basis $b_1, \ldots, b_{2g}$ by the matrix $N$.

The lattice $\Lambda$ has a basis that is *symplectic* with respect to $E$, i.e., a $\mathbf{Z}$-basis $e_1, \ldots, e_g, v_1, \ldots, v_g$ with respect to which $E$ is given by the matrix $\Omega$, given in terms of $(g \times g)$-blocks as

$$\Omega = \begin{pmatrix} 0 & 1_g \\ -1_g & 0 \end{pmatrix}. \tag{4.1}$$

The vectors $v_i$ form a $\mathbf{C}$-basis of $\mathbf{C}^g$ and if we rewrite $\mathbf{C}^g$ and $\Lambda$ in terms of this basis, then $\Lambda$ becomes $Z\mathbf{Z}^g + \mathbf{Z}^g$, where $Z$ is a *period matrix*, i.e., a symmetric matrix over $\mathbf{C}$ with positive definite imaginary part. The set of all $g \times g$ period matrices is called the *Siegel upper half space* and denoted by $\mathcal{H}_g$. It is a topological subspace of the Euclidean $2g^2$-dimensional real vector space $\mathrm{Mat}_g(\mathbf{C})$.

There is an action on this space by the *symplectic group*

$$\mathrm{Sp}_{2g}(\mathbf{Z}) = \{M \in \mathrm{GL}_{2g}(\mathbf{Z}) : M^{\mathrm{t}}\Omega M = \Omega\} \subset \mathrm{GL}_{2g}(\mathbf{Z}),$$

given in terms of $(g \times g)$-blocks by

$$\begin{pmatrix} A & B \\ C & D \end{pmatrix}(Z) = (AZ + B)(CZ + D)^{-1}.$$

The association of $Z$ to $(\mathbf{C}^g/Z\mathbf{Z}^g + \mathbf{Z}^g, E)$ gives a bijection between the set $\mathrm{Sp}_{2g}(\mathbf{Z})\backslash\mathcal{H}_g$ of orbits and the set of principally polarized abelian varieties over $\mathbf{C}$ up to isomorphism. We call this set of orbits the Siegel moduli space.

## 4.1 A symplectic basis for $\Phi(\mathfrak{a})$

Now it is time to compute symplectic bases. In Algorithm 3.1, we computed a set of abelian varieties over $\mathbf{C}$, each given by a triple $(\Phi, \mathfrak{a}, \xi)$, where $\mathfrak{a}$ is an ideal in $\mathcal{O}_K$, given by a basis, $\xi$ is in $K^*$ and $\Phi$ is a CM-type of $K$. We now identify $\mathfrak{a}$ with the lattice $\Lambda = \Phi(\mathfrak{a}) \subset \mathbf{C}^g$ and recall that the bilinear form $E : \mathfrak{a} \times \mathfrak{a} \to \mathbf{Z}$ is given by $E : (x, y) \mapsto \mathrm{Tr}_{K/\mathbf{Q}}(\xi x\overline{y})$. We can write down the matrix $N \in \mathrm{Mat}_{2g}(\mathbf{Z})$ of $E$ with respect to the basis of $\mathfrak{a}$. Computing a symplectic basis of $\mathfrak{a}$ now comes down to computing a change of basis $M \in \mathrm{GL}_{2g}(\mathbf{Z})$ of $\mathfrak{a}$ such that $M^{\mathrm{t}}NM = \Omega$, with $\Omega$ as in (4.1). This is done by the following algorithm.

**Algorithm 4.2.**
**Input:** A matrix $N \in \mathrm{Mat}_{2g}(\mathbf{Z})$ such that $N^{\mathrm{t}} = -N$ and $\det N = 1$.
**Output:** $M \in \mathrm{GL}_{2g}(\mathbf{Z})$ satisfying $M^{\mathrm{t}} N M = \Omega$.

For $i = 1, \ldots, g$, do the following.

1. Let $e_i' \in \mathbf{Z}^{2g}$ be a vector linearly independent of
$$\{e_1, \ldots, e_{i-1}, v_1, \ldots, v_{i-1}\}.$$
2. From $e_i'$, compute the following vector $e_i$, which is orthogonal to $e_1, \ldots, e_{i-1}$, $v_1, \ldots, v_{i-1}$:
$$e_i = \frac{1}{k}\left(e_i' - \sum_{j=1}^{i-1}(e_j^{\mathrm{t}} N e_i')v_j + \sum_{j=1}^{i-1}(v_j^{\mathrm{t}} N e_i')e_j\right),$$
where $k$ is the largest positive integer such that the resulting vector $e_i$ is in $\mathbf{Z}^{2g}$.
3. Let $v_i'$ be such that $e_i^{\mathrm{t}} N v_i' = 1$. We will explain this step below.
4. From $v_i'$, compute the following vector $v_i$, which is orthogonal to $e_1, \ldots, e_{i-1}$, $v_1, \ldots, v_{i-1}$ and satisfies $e_i^{\mathrm{t}} N v_i = 1$:
$$v_i = v_i' - \sum_{j=1}^{i-1}(e_j^{\mathrm{t}} N v_i')v_j + \sum_{j=1}^{i-1}(v_j^{\mathrm{t}} N v_i')e_j.$$

Output the matrix $M$ with columns $e_1, \ldots, e_g, v_1, \ldots, v_g$.

Existence of $v_i'$ as in step 3 follows from the facts that $N$ is invertible and that $e_i \in \mathbf{Z}^{2g}$ is not divisible by integers greater than 1. Actually finding $v_i'$ means finding a solution of a linear equation over $\mathbf{Z}$, which can be done using the LLL-algorithm as in [57, Section 14].

If we apply the Algorithm 4.2 to the matrix $N$ mentioned above it, then the output matrix $M$ is a basis transformation that yields a symplectic basis of $\Lambda$ with respect to $E$. For fixed $g$, Algorithm 4.2 takes time polynomial in the size of the input, hence polynomial time in the bit sizes of $\xi \in K$ and the basis of $\mathfrak{a}$. Lemma 3.6 tells us that for $g = 2$, we can make sure that both $\xi \in K$ and the basis of $\mathfrak{a}$ have a bit size that is polynomial in $\log \Delta$, so obtaining a period matrix $Z$ from a triple $(\Phi, \mathfrak{a}, \xi)$ takes time only polynomial in $\log \Delta$. This implies also that the bit size of $Z$ (as a matrix with entries in a number field) is polynomial in $\log \Delta$.

## 4.2 A symplectic basis for $(z, \mathfrak{b})$

Let $K$ be a quartic CM-field with real quadratic subfield $K_0$ and let $\delta = \sqrt{\Delta_0} \in K_0$.

We have seen in Section I.5.3 that every triple $(\Phi, \mathfrak{a}, \xi)$ as in Section I.5.2 is up to equivalence of the form $\mathfrak{a} = z\mathfrak{b}+\mathfrak{b}^{-1}$, $\xi = (z-\overline{z})^{-1}\delta^{-1}$, $\Phi = \{\phi : K \to \mathbf{C} : \operatorname{Im}\phi\xi > 0\}$.

For a triple in this form, we can give the following explicit symplectic basis. Let $K_0 \to K_0 : x \mapsto x^c$ be the non-trivial automorphism.

**Theorem 4.3.** *Let $K$ be a quartic CM-field and let the notation be as above. Let $b_1, b_2$ be a basis of $\mathfrak{b}$. Then we have $b_1 b_2^c - b_1^c b_2 = sN(\mathfrak{b})\delta$ for some $s \in \{\pm 1\}$.*

*The basis*

$$\Phi(zb_1), \quad \Phi(zb_2), \quad -sN(\mathfrak{b})^{-1}\Phi(b_2^c), \quad sN(\mathfrak{b})^{-1}\Phi(b_1^c)$$

*of $\Phi(\mathfrak{a})$ is symplectic with respect to the polarization corresponding to $\xi$. The period matrix for this symplectic basis is given by*

$$Z = \sum_{i=1}^{2} \phi_i \left( \frac{-z}{\delta} \begin{pmatrix} b_1^2 & b_1 b_2 \\ b_1 b_2 & b_2^2 \end{pmatrix} \right).$$

*Proof.* Let $|\cdot|$ be an archimedean norm on $K_0$. Then $|b_1 b_2^c - b_1^c b_2|$ is the covolume of $\mathfrak{b}$ in $K_0 \otimes \mathbf{R}$, which is $N(\mathfrak{b})\,|\delta|$, hence we have $b_1 b_2^c - b_1^c b_2 = sN(\mathfrak{b})\delta$ with $s \in \{\pm 1\}$. Recall $E(\Phi(u), \Phi(v)) = \operatorname{Tr}_{K/\mathbf{Q}}(\xi\overline{u}v)$. A direct computation shows that the given basis of $\Phi(\mathfrak{a})$ is symplectic for $E$. For example, we have

$$\begin{aligned} E(\Phi(zb_1), -sN(\mathfrak{b})^{-1}\Phi(b_2^c)) &= -sN(\mathfrak{b})^{-1}\operatorname{Tr}_{K/\mathbf{Q}}(\xi\overline{z}b_1 b_2^c) \\ &= -sN(\mathfrak{b})^{-1}\operatorname{Tr}_{K_0/\mathbf{Q}}(\xi(\overline{z}-z)b_1 b_2^c) \\ &= sN(\mathfrak{b})^{-1}\operatorname{Tr}_{K_0/\mathbf{Q}}(\delta^{-1}b_1 b_2^c) \\ &= sN(\mathfrak{b})^{-1}\delta^{-1}(b_1 b_2^c - b_1^c b_2) = 1. \end{aligned}$$

Write $\Phi = \{\phi_1, \phi_2\}$ and note that for all $x \in K_0$, we have $\phi_1(x^c) = \phi_2(x)$ and $\phi_2(x^c) = \phi_1(x)$. The symplectic basis reads

$$\begin{pmatrix} \phi_1(zb_1) \\ \phi_2(zb_1) \end{pmatrix}, \begin{pmatrix} \phi_1(zb_2) \\ \phi_2(zb_2) \end{pmatrix}, \frac{-s}{N(\mathfrak{b})} \begin{pmatrix} \phi_2(b_2) \\ \phi_1(b_2) \end{pmatrix}, \frac{s}{N(\mathfrak{b})} \begin{pmatrix} \phi_2(b_1) \\ \phi_1(b_1) \end{pmatrix}.$$

Let $V \in \operatorname{Mat}_2(\mathbf{C})$ have the first two vectors as columns and $V' \in \operatorname{Mat}_2(\mathbf{R})$ the last two, so $Z = V'^{-1}V$. Then we have

$$\det V' = -(sN(\mathfrak{b})^{-1})^2 \det \begin{pmatrix} \phi_1(b_2^c) & \phi_1(b_1^c) \\ \phi_1(b_2) & \phi_1(b_1) \end{pmatrix} = -sN(\mathfrak{b})^{-1}\phi_1(\delta), \quad \text{so}$$

$$V'^{-1} = \phi_1(\delta)^{-1} \begin{pmatrix} -\phi_1(b_1) & \phi_2(b_1) \\ -\phi_1(b_2) & \phi_2(b_2) \end{pmatrix} = - \begin{pmatrix} \phi_1(b_1\delta^{-1}) & \phi_2(b_1\delta^{-1}) \\ \phi_1(b_2\delta^{-1}) & \phi_2(b_2\delta^{-1}) \end{pmatrix}$$

and hence $Z$ is as in the theorem. □

We will need the determinant of the imaginary part of $Z$ later. We give it now as it can easily be derived from the proof of Theorem 4.3. Indeed with $V$ and $V'$ as in that proof, the matrix $V'$ is real, hence $\operatorname{Im} Z = V'^{-1} \operatorname{Im} V$ and $\det \operatorname{Im} Z = (\det V')^{-1} \det(\operatorname{Im} V)$. We have seen $\det V'$ in the proof and we have

$$\begin{aligned} \det \operatorname{Im} V &= (\operatorname{Im} \phi_1(z))(\operatorname{Im} \phi_2(z)) N(\mathfrak{b}) \phi_1(\delta) \\ &= -|\operatorname{Im}(\phi_1 z) \operatorname{Im}(\phi_2 z)| N(\mathfrak{b}) \phi_1(\delta), \end{aligned}$$

so we get

$$\det Y = |\operatorname{Im}(\phi_1 z) \operatorname{Im}(\phi_2 z)| N(\mathfrak{b})^2. \tag{4.4}$$

# 5 The fundamental domain of the Siegel upper half space

In the genus-1 case, to compute the $j$-invariant of a point $z \in \mathcal{H} = \mathcal{H}_1$, one should first move $z$ to the *fundamental domain* for $\mathrm{SL}_2(\mathbf{Z})$, or at least away from $\operatorname{Im} z = 0$, to get good convergence. We use the term *fundamental domain* loosely, meaning a connected subset $\mathcal{F}$ of $\mathcal{H}_g$ such that every $\mathrm{Sp}_{2g}(\mathbf{Z})$-orbit has a representative in $\mathcal{F}$, and that this representative is unique, except possibly if it is on the boundary of $\mathcal{F}$.

In genus 2, when computing $\theta$-values at a point $Z \in \mathcal{H}_2$, as we will do in Section 7, we move the point to the fundamental domain for $\mathrm{Sp}_4(\mathbf{Z})$.

## 5.1 The genus-1 case

For $g = 1$, the fundamental domain $\mathcal{F} \subset \mathcal{H}$ is the set of $z = x + iy \in \mathcal{H}$ that satisfy

(F1) $-\frac{1}{2} < x \leq \frac{1}{2}$ and

(F2) $|z| \geq 1$.

One usually adds a third condition $x \geq 0$ if $|z| = 1$ in order to make the orbit representatives unique, but we will omit that condition as we allow boundary points of $\mathcal{F}$ to be non-unique in their orbit. To move

$z$ into this fundamental domain, we simply iterate the following until $z = x + iy$ is in $\mathcal{F}$:

$$\begin{array}{ll} 1. & z \leftarrow z + \lfloor -x + \frac{1}{2} \rfloor, \\ 2. & z \leftarrow -\frac{1}{z} \text{ if } |z| < 1. \end{array} \tag{5.1}$$

We will also phrase this procedure in terms of positive definite $(2\times 2)$-matrices $Y \in \mathrm{Mat}_2(\mathbf{R})$, which will come in handy in the genus-2 case. We identify such a matrix

$$Y = \begin{pmatrix} y_1 & y_3 \\ y_3 & y_2 \end{pmatrix}$$

with the positive definite binary quadratic form $f = y_1 X^2 + 2y_3 XY + y_2 Y^2 \in \mathbf{R}[X, Y]$. Let $\phi$ be the map that sends $Y$ to the unique element $z \in \mathcal{H}$ satisfying $f(z, 1) = 0$.

Note that $\mathrm{SL}_2(\mathbf{Z})$ acts on $Y$ via $(U, Y) \mapsto UYU^{\mathrm{t}}$. Now $\phi$ induces an isomorphism of $\mathrm{SL}_2(\mathbf{Z})$-sets from the set of positive definite $(2 \times 2)$-matrices $Y \in \mathrm{Mat}_2(\mathbf{R})$ up to scalar multiplication to $\mathcal{H}$.

Note that $\phi^{-1}(\mathcal{F})$ is the set of matrices $Y$ satisfying

$$-y_1 < 2y_3 \le y_1 \le y_2, \tag{5.2}$$

where the first two inequalities correspond to (F1), and the third inequality to (F2). We say that the matrix $Y$ is $\mathrm{SL}_2(\mathbf{Z})$-reduced if it satisfies (5.2).

We phrase and analyze algorithm (5.1) in terms of the matrices $Y$. Even though we will give some definitions in terms of $Y$, all inequalities and all steps in the algorithm will depend on $Y$ only up to scalar multiplication.

---

**Algorithm 5.3.**
**Input:** A positive definite symmetric $(2 \times 2)$-matrix $Y_0$ over $\mathbf{R}$.
**Output:** $U \in \mathrm{SL}_2(\mathbf{Z})$ and $Y = UY_0U^{\mathrm{t}}$ such that $Y$ is $\mathrm{SL}_2$-reduced.

---

Start with $Y = Y_0$ and $U = 1 \in \mathrm{SL}_2(\mathbf{Z})$ and iterate the following two steps until $Y$ is $\mathrm{SL}_2$-reduced.

1. Let

$$U \leftarrow \begin{pmatrix} 1 & 0 \\ r & 1 \end{pmatrix} U \quad \text{and} \quad Y \leftarrow \begin{pmatrix} 1 & 0 \\ r & 1 \end{pmatrix} Y \begin{pmatrix} 1 & r \\ 0 & 1 \end{pmatrix}$$

for $r = \lfloor -y_3/y_1 + \frac{1}{2} \rfloor$.

2. If $y_1 > y_2$, then let

$$U \leftarrow \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} U \quad \text{and} \quad Y \leftarrow \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} Y \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

Output $U, Y$.

---

We can bound the running time in terms of the *minima* of the matrix $Y_0$. We define the *first and second minima* $m_1(Y)$ and $m_2(Y)$ of a symmetric positive definite $(2 \times 2)$-matrix $Y$ as follows. Let $m_1(Y) = p^{\mathrm{t}} Y p$ be minimal among all column vectors $p \in \mathbf{Z}^2$ different from 0 and let $m_2(Y) = q^{\mathrm{t}} Y q$ be minimal among all $q \in \mathbf{Z}^2$ linearly independent of $p$. Note that the definition of $m_2(Y)$ is independent of the choice of $p$. We call $m_1(Y)$ also simply the *minimum* of $Y$. If $Y$ is $\mathrm{SL}_2$-reduced, then we have

$$m_1(Y) = y_1, \quad m_2(Y) = y_2 \quad \text{and} \quad \frac{3}{4} y_1 y_2 \leq \det Y \leq y_1 y_2,$$

so for every positive definite symmetric matrix $Y$, we have

$$\frac{3}{4} m_1(Y) m_2(Y) \leq \det Y \leq m_1(Y) m_2(Y). \tag{5.4}$$

As we have

$$Y^{-1} = \frac{1}{\det Y} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} Y \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix},$$

it also follows that

$$m_i(Y^{-1}) = \frac{m_i(Y)}{\det Y}, \quad (i \in \{1, 2\}). \tag{5.5}$$

For any matrix $A$, let $|A|$ be the maximum of the absolute values of its entries.

**Lemma 5.6.** *Algorithm 5.3 is correct and takes* $O(\log(|Y_0| / m_1(Y_0)))$ *additions, multiplications, and divisions in* $\mathbf{R}$. *The inequalities*

$$|Y| \leq |Y_0| \quad \textit{and} \quad |U| \leq 2(\det Y_0)^{-1/2} |Y_0|$$

*hold for the output, and also for the values of* $Y$ *and* $U$ *throughout the execution of the algorithm.*

*Proof.* The upper bound $\log(|Y_0|/m_1(Y_0))/\log(3)+2$ on the number of iterations is proven on the last page of Section 7 of [57]. Each iteration consists of an absolutely bounded number of operations in $\mathbf{R}$, which proves our bound on the number of operations.

Next, note that $|Y|$ is decreasing throughout the algorithm. Indeed, step 2 only swaps entries and changes signs, while step 1 decreases $|y_3|$ and leaves $y_1$ and $\det Y = y_1y_2 - y_3^2$ invariant, hence also decreases $|y_2|$. This proves that we have $|Y| \le |Y_0|$ throughout the course of the algorithm.

Now let $C_0 \in \mathrm{Mat}_2(\mathbf{R})$ be such that $C_0C_0^{\mathrm{t}} = Y_0$ holds. Then we have $|C_0| \le |Y_0|^{1/2}$ and hence $\left|C_0^{-1}\right| = |\det C_0|^{-1}\,|C_0| \le (\det Y_0)^{-1/2}\,|Y_0|^{1/2}$. As we have $UC_0(UC_0)^{\mathrm{t}} = Y$, we also have $|UC_0| \le |Y|^{1/2} \le |Y_0|^{1/2}$. Finally, $|U| = \left|UC_0C_0^{-1}\right| \le 2\,|UC_0|\,\left|C_0^{-1}\right| \le 2(\det Y_0)^{-1/2}\,|Y_0|$. □

## 5.2 The fundamental domain for genus two

For genus 2, the *fundamental domain* $\mathcal{F}_2$ is defined to be the set of $Z = X + iY \in \mathcal{H}_2$ for which

(S1) the real part $X = \begin{pmatrix} x_1 & x_3 \\ x_3 & x_2 \end{pmatrix}$ is reduced, i.e., $-\frac{1}{2} \le x_i < \frac{1}{2}$ $(i = 1, 2, 3)$,

(S2) the imaginary part $Y$ is ($\mathrm{GL}_2$-)reduced, i.e., $0 \le 2y_3 \le y_1 \le y_2$, and

(S3) $|\det M^*(Z)| \ge 1$ for all $M \in \mathrm{Sp}_4(\mathbf{Z})$, where $M^*(Z)$ is defined by

$$M^*(Z) = CZ + D \quad \text{for} \quad M = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in \mathrm{Sp}_4(\mathbf{Z}).$$

Every point in $\mathcal{H}_2$ is $\mathrm{Sp}_4(\mathbf{Z})$-equivalent to a point in $\mathcal{F}_2$, and we will compute such a point with Algorithm 5.9 below. This point is unique up to identifications of the boundaries of $\mathcal{F}_2$ as we will see in Lemma 5.20. We call points in $\mathcal{F}_2$ $\mathrm{Sp}_4(\mathbf{Z})$*-reduced*.

Reduction of the real part is trivial and obtained by $X \mapsto X + B$, for a unique $B \in \mathrm{Mat}_2(\mathbf{Z})$. Here $X \mapsto X + B$ corresponds to the action of

$$\begin{pmatrix} 1 & B \\ 0 & 1 \end{pmatrix} \in \mathrm{Sp}_4(\mathbf{Z})$$

on $Z$.

Reduction of the imaginary part is reduction of positive definite symmetric matrices as in Algorithm 5.3, but with the extra condition $y_3 \geq 0$, which can be obtained by applying the $\mathrm{GL}_2(\mathbf{Z})$-matrix

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

It follows that $UYU^{\mathrm{t}}$ is reduced for some $U \in \mathrm{GL}_2(\mathbf{Z})$, and to reduce the imaginary part of $Z$, we replace $Z$ by

$$UZU^{\mathrm{t}} = \begin{pmatrix} U & 0 \\ 0 & (U^{\mathrm{t}})^{-1} \end{pmatrix}(Z). \tag{5.7}$$

Condition (S3) has a finite formulation. Let $\mathfrak{G}$ consist of the 38 matrices

$$\begin{pmatrix} 0 & 0 & -1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & e_1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & e_1 \end{pmatrix}, \quad \begin{pmatrix} 0 & 0 & -1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & -1 & d & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix}, \quad \begin{pmatrix} 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \\ 1 & 0 & e_1 & e_3 \\ 0 & 1 & e_3 & e_2 \end{pmatrix}, \tag{5.8}$$

in $\mathrm{Sp}_4(\mathbf{Z})$, where $d$ ranges over $\{0, \pm 1, \pm 2\}$ and each $e_i$ over $\{0, \pm 1\}$. Gottschling [37] proved that, under conditions (S1) and (S2), condition (S3) is equivalent to the condition

(G) $|\det M^*(Z)| \geq 1 \quad$ for all $M \in \mathfrak{G}$.

Actually, Gottschling went even further and gave a subset of 19 elements of $\mathfrak{G}$ of which he proved that it is minimal such that (G) is equivalent to (S3), assuming (S1) and (S2).

For our purposes of bounding and computing the values of Igusa invariants, it suffices to consider the set $\mathcal{B} \subset \mathcal{H}_2$, given by (S1), (S2), and

(B) $\qquad y_1 \geq \sqrt{3/4}.$

The condition (B) follows immediately from (S1) and $|z_1| \geq 1$, which is equivalent to $|\det(N_0^*(Z))| \geq 1$ for the upper left matrix in (5.8) with $e_1 = 0$, so $\mathcal{B}$ contains $\mathcal{F}_2$.

## 5.3 The reduction algorithm for genus 2

The reduction algorithm that moves $Z \in \mathcal{H}_2$ into $\mathcal{F}_2$ is as follows.

---

**Algorithm 5.9.**
**Input:** $Z_0 \in \mathcal{H}_2$.
**Output:** $Z$ in $\mathcal{F}_2$ and a matrix

$$M = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in \mathrm{Sp}_4(\mathbf{Z})$$

such that we have $Z = M(Z_0) = (AZ_0 + B)(CZ_0 + D)^{-1}$.

---

Start with $Z = Z_0$ and iterate the following 3 steps until $Z$ is in $\mathcal{F}_2$. During the course of the algorithm, keep track of $M \in \mathrm{Sp}_4(\mathbf{Z})$ such that $Z = M(Z_0)$, as we did with $U$ in Algorithm 5.3.

1. Reduce the imaginary part as explained in Section 5.2.
2. Reduce the real part as explained in Section 5.2.
3. Apply $N$ to $Z$ for $N \in \mathfrak{G}$ with $|\det N^*(Z)| < 1$ minimal, if such an $N$ exists.

---

The algorithm that moves $Z \in \mathcal{H}_2$ into $\mathcal{B}$ is exactly the same, but with $\mathcal{F}_2$ replaced by $\mathcal{B}$ everywhere and with $\mathfrak{G}$ replaced by $\{N_0\}$. We will give an analysis of the running time and output of Algorithm 5.9 below. The only property of the subset $\mathfrak{G} \subset \mathrm{Sp}_4(\mathbf{Z})$ that this analysis uses is that it contains $N_0$, hence the analysis is equally valid for the modification that moves points into $\mathcal{B}$.

We will bound the number of iterations by showing that $\det Y$ is increasing and bounded in terms of $Y_0$, that we have an absolutely bounded number of steps with $|y_1| \geq \frac{1}{2}$, and that every step with $|y_1| < \frac{1}{2}$ leads to a doubling of $\det Y$.

**Lemma 5.10.** *For any point $Z \in \mathcal{H}_2$ and any matrix $M \in \mathrm{Sp}_4(\mathbf{Z})$, we have*

$$\det \mathrm{Im}\, M(Z) = \frac{\det \mathrm{Im}\, Z}{|\det M^*(Z)|^2}.$$

*Proof.* In [48, Proof of Proposition 1.1] it is computed that

$$\mathrm{Im}\, M(Z) = (M^*(Z)^{-1})^{\mathrm{t}} (\mathrm{Im}\, Z) M^*(\overline{Z})^{-1}. \tag{5.11}$$

Taking determinants on both sides proves the result. □

Steps 1 and 2 of Algorithm 5.9 do not change $\det Y$, and Lemma 5.10 shows that step 3 increases $\det Y$, so $\det Y$ is increasing throughout the algorithm.

The following result allows us to bound $m_2(Y)$ and $\det Y$ during the algorithm. It is also crucial in Section 6, where we use it to bound the entries of the reduced period matrix.

**Lemma 5.12.** *For any point $Z = X + iY \in \mathcal{H}_2$ and any matrix $M \in \mathrm{Sp}_4(\mathbf{Z})$, we have*

$$m_2(\operatorname{Im} M(Z)) \leq \frac{4}{3} \max\{m_1(Y)^{-1}, m_2(Y)\}.$$

*Proof.* We imitate part of the proof of [48, Lemma 3.1]. If we replace $M$ by

$$\begin{pmatrix} (U^{\mathrm{t}})^{-1} & 0 \\ 0 & U \end{pmatrix} M$$

for $U \in \mathrm{GL}_2(\mathbf{Z})$, then the matrix $(\operatorname{Im} M(Z))^{-1}$ gets replaced by the matrix $U(\operatorname{Im} M(Z))^{-1}U^{\mathrm{t}}$, so we can assume without loss of generality that $(\operatorname{Im} M(Z))^{-1}$ is reduced. By (5.11), we have

$$\begin{aligned} (\operatorname{Im} M(Z))^{-1} &= (CX - iCY + D)Y^{-1}(CX + iCY + D)^{\mathrm{t}} \\ &= (CX + D)Y^{-1}(XC^{\mathrm{t}} + D^{\mathrm{t}}) + CYC^{\mathrm{t}}, \qquad (5.13) \\ \text{where} \quad M &= \begin{pmatrix} A & B \\ C & D \end{pmatrix}. \end{aligned}$$

As the left hand side of (5.13) is reduced, its minimum $m_1$ is its upper left entry. Let $(c_1, c_2, d_1, d_2) \in \mathbf{Z}^4$ be the third row of $M$ and let $c = (c_1, c_2), d = (d_1, d_2) \in \mathbf{Z}^2$. We compute that the upper left entry of (5.13) is $m_1((\operatorname{Im} M(Z))^{-1}) = (cX + d)Y^{-1}(Xc^{\mathrm{t}} + d^{\mathrm{t}}) + cYc^{\mathrm{t}}$.

The matrix $M$ is invertible, so if $c$ is zero, then $d$ is non-zero. As both $Y^{-1}$ and $Y$ are positive definite, this implies that

$$m_1((\operatorname{Im} M(Z))^{-1}) \geq \min\{m_1(Y), m_1(Y^{-1})\}.$$

By (5.4) and (5.5), we get

$$\begin{aligned} m_2(\operatorname{Im} M(Z)) &\leq \frac{4 \det \operatorname{Im} M(Z)}{3m_1(\operatorname{Im} M(Z))} = \frac{4}{3m_1((\operatorname{Im} M(Z))^{-1})} \\ &\leq \frac{4}{3} \max\{\frac{1}{m_1(Y)}, \frac{\det Y}{m_1(Y)}\} \\ &\leq \frac{4}{3} \max\{m_1(Y)^{-1}, m_2(Y)\}, \end{aligned}$$

which proves the result. □

**Lemma 5.14.** *There is an absolute upper bound $c$, independent of the input $Z_0$, on the number of iterations of Algorithm 5.9 in which $Z$ satisfies $y_1 \geq \frac{1}{2}$ at the beginning of step 3.*

*Proof.* Let $\mathcal{C}$ be the set of points in $\mathcal{H}_2$ that satisfy (S1), (S2) and $y_1 \geq \frac{1}{2}$. At the beginning of step 3, both (S1) and (S2) hold, so we need to bound the number of iterations for which $Z$ is in $\mathcal{C}$ at the beginning of step 3. Suppose that such an iteration exists, and denote the value of $Z$ at the beginning of step 3 of that iteration by $Z'$. As $\det Y$ increases during the algorithm, each iteration has a different value of $Z$, so it suffices to bound the number of $Z \in \mathrm{Sp}_4(\mathbf{Z})(Z') \cap \mathcal{C}$. By [48, Theorem 3.1], the set

$$\mathfrak{C} = \{M \in \mathrm{Sp}_4(\mathbf{Z}) : \mathcal{C} \cap M(\mathcal{C}) \neq \emptyset\}$$

is finite. As $\mathfrak{C}$ surjects onto $\mathrm{Sp}_4(\mathbf{Z})(Z') \cap \mathcal{C}$ via $M \mapsto M(Z')$, we get the absolute upper bound $\#\mathfrak{C}$ on the number of iterations with $Z \in \mathcal{C}$. □

**Lemma 5.15.** *At every iteration of step 3 of Algorithm 5.9 in which we have $y_1 < \frac{1}{2}$, the value of $\det Y$ increases by a factor of at least 2.*

*Proof.* If $y_1 < \frac{1}{2}$, then for the element $N_0 \in \mathfrak{G}$, we have $|\det N_0^*(Z)|^2 = |z_1|^2 = |x_1|^2 + |y_1|^2 \leq \frac{1}{2}$, so by Lemma 5.10, the value of $\det Y$ increases by a factor $\geq 2$. □

We can now bound the number of iterations. For any matrix $Z = X + iY \in \mathcal{H}_2$, let $t(Z) = \log \max\{m_1(Y)^{-1}, m_2(Y)\}$.

**Proposition 5.16.** *The number of iterations of Algorithm 5.9 is at most $O(t(Z_0))$ for every input $Z_0$.*

*Proof.* Let $c$ be the constant of Lemma 5.14, let $Z_0$ be the input of Algorithm 5.9 and let $Z$ be the value after $k$ iterations. By Lemmas 5.15 and 5.12, we have

$$2^{k-c} \det Y_0 \leq \det Y \leq m_2(Y)^2 \leq (\frac{4}{3})^2 \max\{m_1(Y_0)^{-2}, m_2(Y_0)^2\},$$

hence (5.4) implies

$$2^{k-c} \leq (\frac{4}{3})^3 \max\{m_1(Y_0)^{-3} m_2(Y_0)^{-1}, m_1(Y_0)^{-1} m_2(Y_0)\}. \qquad \square$$

To avoid a laborious error analysis, all computations are performed inside some number field $L \subset \mathbf{C}$ of absolutely bounded degree. Indeed, for an abelian surface $A$ with CM by $\mathcal{O}_K$, any period matrix $Z \in \mathcal{H}_2$ that represents $A$ is in $\mathrm{Mat}_2(L)$, where $L$ is the normal closure of $K$,

which has degree at most 8. For a running time analysis, we need to bound the *height* of the numbers involved. Such height bounds are also used for lower bounds on the off-diagonal part of the output $Z$, which we will need in Section 7.

The height $h(x)$ of an element $x \in L^*$ is defined as follows. Let $S$ be the set of absolute values of $L$ that extend either the standard archimedean absolute value of $\mathbf{Q}$ or one of the non-archimedean absolute values $|x| = p^{-\mathrm{ord}_p(x)}$. For each $v \in S$, let $\deg(v) = [L_v : \mathbf{Q}_v]$ be the degree of the completion $L_v$ of $L$ at $v$. Then

$$h(x) = \sum_v \deg(v) \max\{\log |x|_v, 1\}.$$

We denote the maximum of the heights of all entries of a matrix $Z \in \mathcal{H}_2$ by $h(Z)$.

Next, we give bounds on the value of $|M|$ during the execution of the algorithm. This will provide us with a bound on the height of the entries of $Z$. Indeed, if we have $Z = M(Z_0)$, then it follows that $h(Z) \leq 2(\log |M| + h(Z_0) + \log 4)$.

**Lemma 5.17.** *There exists an absolute constant $c > 0$ such that the following holds. The value of $\log |M|$ is at most $c \max\{\log |Z_0|, 1\}$ during the first iteration of Algorithm 5.9 and, in each iteration, increases by at most $c \max\{t(Z_0), 1\}$, where $t$ is as above Proposition 5.16.*

*Proof.* For step 1, it follows from equation (5.7) and Lemma 5.6 that the value of $\log |M|$ increases by at most $\log |Z| + t(Z) + \log 8$. In step 2, the value of $\log |M|$ increases by at most $\log(1 + 2|Z|)$. In step 3, the value of $\log |M|$ increases by at most $\log 4$ by the definition of $\mathfrak{G}$.

Therefore, it suffices to bound $\log |Z|$ appropriately at the beginning of steps 1 and 2. Note that $\log |Y|$ decreases during step 1, while $\log |X|$ increases by at most $\max\{\log |Z|, 0\} + \log 16$. Therefore, it suffices to give a bound for $\log |Z|$ only at the beginning of step 1. Note that for the first iteration, the bound $\log |Z| = \log |Z_0|$ suffices.

At the beginning of step 3, we have $|x_i| \leq \frac{1}{2}$, and $Y$ is reduced. We can thus use Lemma 5.12 to bound the coefficients of $Y$, and get $|Y| \leq 4e^{t(Z_0)}/3$. This proves that we have $\log |Z| \leq 3 \max\{t(Z_0), 1\}$. During step 3, the matrix $Z$ gets replaced by

$$\begin{aligned} N(Z) &= (AZ + B)(CZ + D)^{-1} \\ &= \tfrac{1}{\det(CZ+D)} (AZ + B) \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} (CZ + D) \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \end{aligned}$$

where

$$N = \begin{pmatrix} A & B \\ C & D \end{pmatrix}$$

is in the set $\mathfrak{G}$. We have $|N(Z)| \leq |\det(CZ+D)|^{-1}(2|Z|+1)^2|N|^2$. We have already bounded $|Z|$, and we also have $|N| \leq 4$, so we only need to bound $|\det(CZ+D)|^{-1}$. Lemma 5.10 gives

$$|\det(CZ+D)|^{-2} = (\det \operatorname{Im} N(Z))(\det \operatorname{Im}(Z))^{-1}.$$

Let $M'$ be such that we have $Z = M'(Z_0)$ and let $M = NM'$, then Lemma 5.12 tells us that the numerator is at most

$$4\max\{m_1(Y_0)^{-1}, m_2(Y_0)\}/3.$$

Applying the fact that the determinant of $\operatorname{Im}(Z)$ increases during the execution of the algorithm, we thus find

$$|\det(CZ+D)|^{-2} = 4\max\{m_1(Y_0)^{-1}, m_2(Y_0)\}/(3\det \operatorname{Im}(Z_0)),$$

which is at most $16/9\max\{m_1(Y_0), m_2(Y_0)\}^3$ by (5.4). Therefore, for $Z$ and $N$ as in step 3, we have $\log|N(Z)| = c'\max\{t(Z_0),1\}$, hence we find that $c'\max\{t(Z_0),1\}$ is an upper bound for $\log|Z|$ at the beginning of step 1 for every iteration but the first. □

**Theorem 5.18.** *Let $L \subset \mathbf{C}$ be a number field. Algorithm 5.9, on input $Z_0 \in \operatorname{Mat}_2(L) \cap \mathcal{H}_2$, returns an $\operatorname{Sp}_4(\mathbf{Z})$-equivalent matrix $Z \in \mathcal{F}_2$. The running time is $\widetilde{O}(h(Z_0)\log|Z_0|) + \widetilde{O}(t(Z_0)^4)$. Moreover, the output $Z$ satisfies*

$$h(Z) = c'\max\{h(Z_0), t(Z_0)^2, 1\},$$

*for some absolute constant $c'$.*

*Proof.* By Proposition 5.16 and Lemma 5.17, the value of $\log|M|$ is bounded by $O(\log|Z_0|) + O(t(Z_0)^2)$ throughout the algorithm, so the height of every entry of $Z$ is bounded by $O(t(Z_0)^2) + O(h(Z_0))$. This implies that each basic arithmetic operation in the algorithm takes time at most $\widetilde{O}(t(Z_0)^2) + \widetilde{O}(h(Z_0))$. By Lemma 5.6, the first iteration takes $O(\log|Z_0|) + O(t(Z_0))$ such operations, and all other $O(t(Z_0))$ iterations take $O(t(Z_0))$ operations, so there are $O(\log|Z_0|) + O(t(Z_0)^2)$ arithmetic operations, yielding a total running time for the algorithm of $\widetilde{O}(t(Z_0)^4) + \widetilde{O}(h(Z_0)\log|Z_0|)$ □

In Section 7, we bound the Igusa invariants in terms of the entries of the period matrix $Z$. One of the bounds that we need in that section is a lower bound on the absolute value of the off-diagonal entry $z_3$ of $Z$. It is supplied by the following corollary.

**Corollary 5.19.** Let $Z_0 \in \mathrm{Mat}_2(L) \cap \mathcal{H}_2$ be the input of Algorithm 5.9 and let $z_3$ be the off-diagonal entry of the output. Then either $z_3$ is zero or we have $-\log|z_3| \leq c' \max\{h(Z_0), t(Z_0)^2, 1\}$ for an absolute constant $c'$.

*Proof.* The field $L$ is a subfield of $\mathbf{C}$, which gives us a standard absolute value $v$. If $z_3$ is non-zero, then the product formula tells us that we have $-\log|z_3| = -\log|z_3|_v = \sum_{w \neq v} \log|z_3|_w \leq h(z_3)$, which is at most $c' \max\{h(Z_0), t(Z_0)^2, 1\}$ by Theorem 5.18. □

## 5.4 Identifying points on the boundary

Now that we know how to move points to the fundamental domain $\mathcal{F}_2$, the following lemma shows how to see if two points in $\mathcal{F}_2$ are $\mathrm{Sp}_4(\mathbf{Z})$-equivalent. Using this lemma, one could, for example, eliminate duplicate abelian varieties if one chooses to use a non-proven alternative method for the class group computations in Algorithm 3.1. We do not need this lemma for the proof of the main theorem.

**Lemma 5.20.** *For every element $Z$ of $\mathcal{F}_2$, the set $\mathrm{Sp}_4(\mathbf{Z})(Z) \cap \mathcal{F}_2$ can be computed as follows.*

1. *Let $S_3 = \{N(Z) \in \mathcal{H}_2 \mid N \in \mathfrak{G}, |\det N^*(Z)| = 1\}$.*
2. *For $Z''' \in S_3$, let $S_{Z'''}$ be the set of $U \in \mathrm{GL}_2(\mathbf{Z})/\{\pm 1\}$ such that $UZ'''U^{\mathrm{t}}$ satisfies (S2).*

   *We can compute $S_{Z'''}$ as follows.*

   (a) *Let $U$ be one element of $S_{Z'''}$, which can be found using $\mathrm{GL}_2(\mathbf{Z})$-reduction of $\operatorname{Im} Z'''$ as explained in Section 5.2, and let $Y = UZ'''U^{\mathrm{t}}$.*

   (b) *Write*

$$Y = \begin{pmatrix} y_1 & y_3 \\ y_3 & y_2 \end{pmatrix} \in \mathrm{Mat}_2(\mathbf{R})$$

   *and let $G \subset \mathrm{GL}_2(\mathbf{Z})/\{\pm 1\}$ be the stabilizer of $Y$, which is given as follows. Let $V$ be the subset of $\mathrm{GL}_2(\mathbf{Z})$ that contains*

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \text{if and only if} \quad y_1 = y_2,$$

$$\begin{pmatrix} 1 & -1 \\ 0 & -1 \end{pmatrix} \quad \text{if and only if} \quad 2y_3 = y_1,$$

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad \text{if and only if} \quad y_3 = 0,$$

*and no other elements, so $V$ has 0, 1, or 2 elements. Then we have $G = \langle V\rangle \subset \mathrm{GL}_2(\mathbf{Z})/\{\pm 1\}$, which has order 1, 2, 4, or 6.*

*(c) We have $S_{Z'''} = GU$.*

*Let $S_2 = \{UZ'''U^{\mathrm{t}} \mid Z''' \in S_1, U \in S_{Z'''}\}$.*

3. *Let $S_1 = \{Z'' + T(Z'') \in \mathcal{H}_2 \mid Z'' \in S_2\}$, where $T(Z'') \in \mathrm{Mat}_2(\mathbf{Z})$ is the unique matrix such that $Z' = Z'' + T(Z'')$ satisfies (S1).*

*We have $S_1 = \mathrm{Sp}_4(\mathbf{Z})(Z) \cap \mathcal{F}_2$.*

*Proof.* Let $Z'$ be an element of $S_1$ and let $M \in \mathrm{Sp}_4(\mathbf{Z})$ be the matrix

$$M = \begin{pmatrix} 1 & T \\ 0 & 1 \end{pmatrix} \begin{pmatrix} U & 0 \\ 0 & (U^{\mathrm{t}})^{-1} \end{pmatrix} N, \tag{5.21}$$

where $N$, $U$, and $T = T(Z'')$ are as in steps 1, 2, and 3, hence we have $M(Z) = Z'$. By construction, $Z'$ is $\mathrm{Sp}_4(\mathbf{Z})$-equivalent to $Z$ and satisfies (S1) and (S2). Moreover, we have $|\det M^*(Z)| = |\det N^*(Z)| = 1$, and $Z$ satisfies (S3), so for any $M' \in \mathrm{Sp}_4(\mathbf{Z})$, we compute

$$|\det M'^*(Z')| = |\det(M'M)^*(Z)|\,|\det M^*(Z)|^{-1} \geq 1.$$

Therefore, $Z'$ also satisfies (S3) and we have $S_1 \subset \mathrm{Sp}_4(\mathbf{Z})(Z) \cap \mathcal{F}_2$.

Conversely, let $M \in \mathrm{Sp}_{2g}(\mathbf{Z})$ be such that $M(Z)$ is in $\mathcal{F}_2$. For any $M' \in \mathrm{Sp}_4(\mathbf{Z})$, let $l(M')$ be the lower half of $M'$, i.e., the $(2 \times 4)$-matrix having as rows the third and fourth row of $M'$. As both $Z$ and $M(Z)$ lie in $\mathcal{F}_2$, we have $|\det M^*(Z)| = 1$, and $Z$ satisfies (S1), (S2), and $|z_1|, |z_2| \geq 1$. The proof of [37, Satz 1] shows that this implies that we have $l(M) = (U^{\mathrm{t}})^{-1} l(N)$ for some $U \in \mathrm{GL}_2(\mathbf{Z})$ and some $N \in \mathfrak{G}$.

Now $M$ and

$$\begin{pmatrix} U & 0 \\ 0 & (U^{\mathrm{t}})^{-1} \end{pmatrix} N$$

are symplectic matrices with the same lower half, and this implies that (5.21) holds for some symmetric integer matrix $T$. In particular, the matrix

$$U(\operatorname{Im} N(Z))U^{\mathrm{t}} = \operatorname{Im} M(Z)$$

satisfies (S2), hence $Z'' = U(N(Z))U^{\mathrm{t}}$ is an element of $S_2$. Finally, by uniqueness of $T(Z'')$, we have $T = T(Z'')$ and hence $M(Z)$ is an element of $S_1$.

It remains to show that the set $S_{Z'''}$ computed in steps a–c is correct. This follows from the fact that if both $UYU^{\mathrm{t}}$ and $Y$ are reduced, then $(U \bmod \pm 1)$ is in the stabilizer $G$ of $Y$. □

# 6 Bounds on the period matrices

This section is needed only for the proof of the runtime bound of our algorithm, not for the algorithm itself. In Sections 3 – 5, we gave an algorithm that computes one period matrix $Z$ in the fundamental domain $\mathcal{F}_2$ of the Siegel upper half space $\mathcal{H}_2$ for every isomorphism class of principally polarized abelian surface over $\mathbf{C}$ with CM by $\mathcal{O}_K$. In Section 7, we give bounds on the Igusa invariants in terms of the minima of $\operatorname{Im} Z$. The purpose of the current section is therefore to bound these minima. The main result is Corollary 6.2 below.

## 6.1 The bound on the period matrix

The period matrix $Z$ was computed via a reduction algorithm, starting from the fairly arbitrary period matrix obtained in Algorithm 4.2. As a result, we are unable to obtain optimal bounds via an analysis of the way $Z$ was computed. Instead, use a period matrix $Z'$ coming from a pair $(z, \mathfrak{b})$ as in Section I.5.3 on which we can get certain bounds, and transfer those bounds to $Z$ using Lemma 5.12. Working directly with the period matrix $Z'$ instead of $Z$ in our algorithms is not an option, because $Z'$ will not always be in the fundamental domain $\mathcal{F}_2$, where Section 7 needs it to be.

The bounds on $Z$ and $Z'$ are given by the following two results. For a quartic CM-field $K$, let $\Delta$ be the discriminant of $K$ and let $\Delta_0$ be the discriminant of its real quadratic subfield $K_0$, so we have $\Delta = \Delta_1 \Delta_0^2$, where $\Delta_1$ is the norm of the relative discriminant of $K/K_0$.

**Proposition 6.1.** *Let $K$ be a primitive quartic CM-field. Every principally polarized abelian surface with complex multiplication by $\mathcal{O}_K$ has a symplectic basis for which the period matrix $Z' = X' + iY'$ satisfies*

$$\frac{\pi^2}{6\Delta_0} \leq \det Y' \leq \frac{\Delta_1^{1/2}}{4} \quad \textit{and}$$

$$\frac{2\pi}{\sqrt{6}\Delta_0} \leq m_1(Y') \leq m_2(Y') \leq \frac{\Delta_1^{1/4}\Delta_0^{1/2}}{3}.$$

We will prove Proposition 6.1 later.

**Corollary 6.2.** Let $K$ be a primitive quartic CM-field and let $Z$ be any period matrix corresponding to a principally polarized abelian surface with CM by $\mathcal{O}_K$. Then we have

$$m_2(\operatorname{Im} Z) \leq \max\left\{\frac{2\sqrt{2}}{\sqrt{3}\pi}\Delta_0, \frac{4}{9}\Delta_1^{1/4}\Delta_0^{1/2}\right\}.$$

*Proof of Corollary 6.2.* Any such period matrix $Z$ can be obtained via $\mathrm{Sp}_4(\mathbf{Z})$-transformation from the matrix $Z'$ of Proposition 6.1. Lemma 5.12 bounds the second minimum $m_2(\operatorname{Im} Z)$ in terms of the minima of $Y'$:

$$m_2(\operatorname{Im} Z) \le \frac{4}{3}\max\{m_1(Y')^{-1}, m_2(Y')\}. \qquad \square$$

## 6.2 A good pair $(z, \mathfrak{b})$

Let $K$ be a primitive quartic CM-field and let $(z, \mathfrak{b})$ be a pair as in Section I.5.3, so $z$ is an element of $K$ and $\mathfrak{b}$ is a fractional ideal in $K_0$. Let $I(z) = \prod_\phi |\operatorname{Im} \phi z|$, where the product ranges over the embeddings $\phi : K \to \mathbf{C}$ up to complex conjugation, so $I(z)^2 = N_{K/\mathbf{Q}}(\frac{1}{2}(z - \overline{z}))$.

The following lemma bounds the consecutive minima of the imaginary part of the period matrix corresponding to the symplectic basis of Theorem 4.3.

**Lemma 6.3.** *Let $(z, \mathfrak{b})$ be as in Section I.5.3. Let $Z = X + iY$ be the period matrix corresponding to the symplectic basis of Theorem 4.3. Then we have* $\det Y = I(z)N(\mathfrak{b})^2$ *and*

$$\frac{2}{\Delta_0^{1/2}} N(\mathfrak{b}) I(z)^{1/2} \le m_1(Y) \le m_2(Y) \le \frac{2\Delta_0^{1/2}}{3} N(\mathfrak{b}) I(z)^{1/2}.$$

*Proof.* The period matrix is given by

$$Z = \sum_{i=1}^{2} \phi_i \left( \frac{z}{\delta} \begin{pmatrix} b_1^2 & b_1 b_2 \\ b_1 b_2 & b_2^2 \end{pmatrix} \right)$$

for some basis $b_1, b_2$ of $\mathfrak{b}$. Let $Y = \operatorname{Im} Z$. Recall that the first minimum $m_1(Y)$ of $Y$ is the minimal value of $(m,n)Y(m,n)^{\mathrm{t}}$ for $(m,n) \in \mathbf{Z}^2 \setminus \{(0,0)\}$. Let $t = mb_1 + nb_2 \in \mathfrak{b}^{-1}$. Then we have

$$\begin{aligned} (m,n)Y(m,n)^{\mathrm{t}} &= \operatorname{Im}(\phi_1(zt^2\delta^{-1})) + \operatorname{Im}(\phi_2(zt^2\delta^{-1})) \\ &\ge 2I(zt^2\delta^{-1})^{1/2} \\ &= 2I(z)^{1/2}\Delta_0^{-1/2} \left| N_{K_0/\mathbf{Q}}(t) \right|. \end{aligned}$$

As we have $\left|N_{K_0/\mathbf{Q}}(t)\right| \ge N(\mathfrak{b})$ for $t \ne 0$, we get

$$m_1(Y) \ge 2N(\mathfrak{b})\Delta_0^{-1/2} I(z)^{1/2}.$$

The determinant of $Y$ is given in (4.4). Finally, the inequality $m_1(Y)m_2(Y) \le \frac{4}{3}\det Y$ gives the upper bound on $m_2(Y)$. $\square$

To prove Proposition 6.1, we need to find a pair $(z, \mathfrak{b})$ for which we have both a good upper and a good lower bound on $I(z)N(\mathfrak{b})^2$. We first give an upper bound that holds for every pair $(z, \mathfrak{b})$. Then we show how to find $(z, \mathfrak{b})$ such that $I(z)N(\mathfrak{b})^2$ is large and we give a lower bound on $I(z)N(\mathfrak{b})^2$ for that particular pair.

**Lemma 6.4.** *Let $K$ be a quartic CM-field with real quadratic subfield $K_0$. Suppose that $z\mathfrak{b} + \mathfrak{b}^{-1}$ is an $\mathcal{O}_K$-submodule of $K$ for $z \in K$ and $\mathfrak{b}$ a fractional $\mathcal{O}_{K_0}$-ideal. Then $(z - \overline{z})\mathfrak{b}^2\mathcal{O}_K$ contains the relative different $\mathcal{D}_{K/K_0} \subset \mathcal{O}_K$. Moreover, we have $I(z)N(\mathfrak{b})^2 \leq 2^{-2}\Delta_1^{1/2}$.*

*Proof.* For any $\alpha \in \mathcal{O}_K$, we have $\alpha w \in z\mathfrak{b} + \mathfrak{b}^{-1}$ for all $w \in \mathfrak{b}^{-1}$. Therefore, we have $\alpha = uz + v$ with $u \in \mathfrak{b}^2$ and $v \in \mathcal{O}_{K_0}$. We thus find that $\alpha - \overline{\alpha} = u(z - \overline{z})$ is in $(z - \overline{z})\mathfrak{b}^2$ for all $\alpha \in \mathcal{O}_K$. The set of all $\alpha - \overline{\alpha}$ as $\alpha$ ranges over $K$ generates the relative different $\mathcal{D}_{K/K_0}$ as an $\mathcal{O}_K$-ideal, which proves the inclusion of ideals.

Taking the norm $N_{K/\mathbf{Q}}$ of this inclusion, we find that the fractional $\mathbf{Q}$-ideal $(2^4 I(z)^2 N_{K_0/\mathbf{Q}}(\mathfrak{b})^4)$ contains $(\Delta_1)$. The square root of this is the bound. □

The following lemma gives the lower bound.

**Lemma 6.5.** *Let $K$ be a quartic CM-field and $K_0$ its real quadratic subfield. Let $\delta = \sqrt{\Delta_0}$ be a generator of the different of $K_0$.*

*Every pair $(z', \mathfrak{b}')$ such that $z'\mathfrak{b}' + \mathfrak{b}'^{-1}$ is an $\mathcal{O}_K$-ideal is equivalent to a pair $(z, \mathfrak{b})$ with*

$$I(z)N(\mathfrak{b})^2 \geq I(z) \geq \frac{\pi^2}{6}\Delta_0^{-1}.$$

*Proof.* By Theorems I.5.8 and I.5.9, we can assume $\mathfrak{b}' = \mathcal{O}_{K_0}$. Identify $\mathfrak{a}' = z'\mathcal{O}_{K_0} + \mathcal{O}_{K_0}$ with its image $\Phi(\mathfrak{a}')$ inside $\mathbf{C}^g$. Then $\mathfrak{a}'$ is a lattice of covolume $\Delta_0 I(z')$. For $B \geq 0$, define the set $S$ by

$$S = \{z \in \mathbf{C}^2 \mid \sum_{i=1}^{2} |z_i| \leq B^{\frac{1}{4}}\} \subset \mathbf{C}^g.$$

Then $S$ has volume $BC$ with $C = \pi^2/6$. Take $B = 2^4 C^{-1}\Delta_0 I(z')$, so that by Minkowski's convex body theorem, there exists a non-zero element $y = bz' + d \in \mathfrak{a}' \cap S$ with $b, d \in \mathcal{O}_{K_0}$. As we have $y \in S$, we find $\prod_{i=1}^{2} |\phi_i(y)| \leq (\frac{1}{2}\sum_{i=1}^{2} |\phi_i(y)|)^2 \leq 2^{-2}B^{1/2}$.

Let $\mathfrak{b} = b\mathcal{O}_{K_0} + d\mathcal{O}_{K_0} \subset \mathcal{O}_{K_0}$, choose $a, c \in \mathfrak{b}^{-1} \subset K_0$ such that $ad - bc = 1$, and let

$$z = \frac{az' + c}{y} = \frac{az' + c}{bz' + d}, \quad \mathfrak{a} = z\mathfrak{b} + \mathfrak{b}^{-1}, \quad \text{and} \quad \xi = (z - \overline{z})^{-1}\delta^{-1}.$$

Then we have $\mathfrak{a} = y^{-1}\mathfrak{a}'$ and $\xi = y\overline{y}\xi'$, so $(\Phi, \mathfrak{a}, \xi)$ is equivalent to $(\Phi, \mathfrak{a}', \xi')$, hence $(z, \mathfrak{b})$ is equivalent to $(z', \mathcal{O}_{K_0})$.

For $i = 1, 2$, we now have (with $y = bz' + d$ and using $ad - bc = 1$)

$$\operatorname{Im} \phi_i z = \operatorname{Im} \phi_i \frac{az' + c}{y} = \frac{\operatorname{Im} \phi_i z'}{|\phi_i y|^2}.$$

Taking the product over all $i$, we find

$$I(z) \geq B^{-1} 2^4 I(z') \geq \pi^2/(6\Delta_0).$$

Note that we have $N(\mathfrak{b}) \geq 1$, hence the bounds in the lemma follow. □

*Proof of Proposition 6.1.* Given a principally polarized CM abelian surface $A$, let $z \in K$ and the ideal $\mathfrak{b} \subset \mathcal{O}_{K_0}$ be as in Lemma 6.5. By Lemmas 6.4 and 6.5, we have

$$\frac{\pi^2}{6}\Delta_0^{-1} \leq I(z) N(\mathfrak{b})^2 \leq \frac{1}{4}\Delta_1^{1/2}.$$

Let $Z$ be the period matrix corresponding to the symplectic basis of Theorem 4.3. Then Lemma 6.3 proves the bounds that we need to prove. □

**Remark 6.6.** The lower bound of Lemma 6.5 is in fact something that holds in greater generality: in the language of the Hilbert upper half space from Remark I.5.10, this lower bound is Lemma 2.2 of [86] and tells us something about the 'floors' of the fundamental domain for the action of $\mathrm{SL}_2(\mathcal{O}_{K_0})$.

# 7 Theta constants

To compute the absolute Igusa invariants corresponding to a point $Z \in \mathcal{H}_2$, we use *theta constants*, also known as *theta null values*. For $z \in \mathbf{C}$, let $E(z) = e^{\pi i z}$. We call an element $c \in \{0, \frac{1}{2}\}^4$ a *theta characteristic* and write $c = (c_1, c_2, c_3, c_4)$, $c' = (c_1, c_2)$ and $c'' = (c_3, c_4)$. We define the *theta constant of characteristic* $c$ to be the function $\theta[c] : \mathcal{H}_2 \to \mathbf{C}$ given by

$$\theta[c](Z) = \sum_{n \in \mathbf{Z}^2} E((n + c')Z(n + c')^{\mathrm{t}} + 2(n + c')c''^{\mathrm{t}}),$$

and following Dupont [20], we use the short-hand notation

$$\theta_{16c_2 + 8c_1 + 4c_4 + 2c_3} = \theta[c].$$

We call a theta characteristic — and the corresponding theta constant — even or odd depending on whether $4c'c''^{\mathrm{t}}$ is even or odd. The odd theta constants are zero by the anti-symmetry in the definition, and there are exactly 10 even theta constants $\theta_0, \theta_1, \theta_2, \theta_3, \theta_4, \theta_6, \theta_8, \theta_9, \theta_{12}$ and $\theta_{15}$.

## 7.1 Igusa invariants in terms of theta constants

Let $T$ be the set of even theta characteristics and define

$$S = \{C \subset T \mid \#C = 4, \sum_{c \in C} c \in \mathbf{Z}^4\}.$$

Then $S$ consists of 15 subsets of $T$ called *Göpel quadruples*, each consisting of 4 even theta characteristics. We call a set $\{b, c, d\} \subset T$ of three distinct even theta characteristics *syzygous* if it is a subset of a Göpel quadruple, so there are 60 syzygous triples. Define

$$\begin{aligned} h_4 &= \sum_{c \in T} \theta[c]^8, \\ h_6 &= \sum_{\substack{b,c,d \in T \\ \text{syzygous}}} \pm(\theta[b]\theta[c]\theta[d])^4 \\ h_{10} &= \prod_{c \in T} \theta[c]^2, \\ h_{12} &= \sum_{C \in S} \prod_{c \in T \setminus C} \theta[c]^4, \end{aligned} \tag{7.1}$$

where we explain the signs in $h_6$ below. Each $h_k$ is a sum of $t_k$ monomials of degree $2k$ in the 10 even theta constants, where $t_4 = 10$, $t_6 = 60$, $t_{10} = 1$, and $t_{12} = 15$. The signs in $h_6$ are defined uniquely by the facts that $h_6$ is a modular form for $\mathrm{Sp}_4(\mathbf{Z})$ and that the coefficient of

$$\Big(\theta[0,0,0,0] \;\; \theta[0,0,0,\tfrac{1}{2}] \;\; \theta[0,0,\tfrac{1}{2},0]\Big)^4$$

is $+1$. More explicitly, the coefficient of

$$\Big(\theta[b_1,b_2,b_3,b_4] \;\; \theta[c_1,c_2,c_3,c_4] \;\; \theta[d_1,d_2,d_3,d_4]\Big)^4$$

is $-1$ to the power

$$\begin{aligned} &b_1 + b_2 + c_1 + c_2 + d_1 + d_2 + b_1c_1 + b_2c_2 + b_4c_2 + b_1c_3 - b_2c_4 + \\ &b_1d_1 - b_3d_1 + c_1d_1 + b_2d_2 + c_2d_2 + c_4d_2 + c_1d_3 - b_2b_3c_1 + \\ &-b_2b_4c_2 - b_1b_2c_3 - b_2b_3d_1 - b_3c_1d_1 - b_1c_3d_1 - b_2c_3d_1 - b_2b_4d_2 + \\ &-b_4c_2d_2 - b_1b_2d_3 - b_1c_1d_3 - b_2c_1d_3. \end{aligned}$$

To compute and check this rule for the sign, we used the action of $\mathrm{Sp}_4(\mathbf{Z})$ on the squares of the theta constants, as made explicit by Dupont [20, Section 6.3.1].

**Remark 7.2.** Another way of defining $h_k$ is as follows. Define Eisenstein series on the $2 \times 2$ Siegel upper half space $\mathcal{H}$ by

$$\psi_k(Z) = \sum_{C,D} \det(CZ + D)^{-k},$$

where the sum is taken over the set of bottom halves $(C, D)$ of elements of $\mathrm{Sp}_4(\mathbf{Z})$ up to left multiplication by $\mathrm{SL}_2(\mathbf{Z})$. Next, define

$$\chi_{10} = -43867(2^{12}3^5 5^2 7 \cdot 53)^{-1}(\psi_4\psi_6 - \psi_{10})$$
$$\chi_{12} = 131 \cdot 593(2^{13}3^7 5^3 7^2 337)^{-1}(3^2 7^2 \psi_4^3 + 2 \cdot 5^3 \psi_6^2 - 691\psi_{12}).$$

Then we have $h_4 = 2^2\psi_4, h_6 = 2^2\psi_6, h_{10} = -2^{14}\chi_{10}$, and $h_{12} = 2^{17}3\chi_{12}$. See also Igusa [46, p. 189] and [47, p. 848].

**Lemma 7.3.** *Let $Z$ be a point in $\mathcal{H}_2$. If $h_{10}(Z)$ is non-zero, then the principally polarized abelian variety corresponding to $Z$ is the Jacobian of a curve $C/\mathbf{C}$ of genus 2 with invariants*

$$I_2(C) = h_{12}(Z)/h_{10}(Z),$$
$$I_4(C) = h_4(Z),$$
$$I_6'(C) = h_6(Z),$$
$$I_{10}(C) = h_{10}(Z).$$

*Proof.* This is the result on page 848 of Igusa [47]. Earlier results of this form are due to Bolza [5]. □

**Remark 7.4.** Thomae's formula ([65, Thm. IIIa.8.1], [85]) gives an equation for a curve $C$ with $J(C)$ corresponding to $Z$ in terms of the theta constants. Formulas of the form of Lemma 7.3 can be derived by writing out the definition of $I_k$ using Thomae's formula and using standard identities between the theta constants. This was done by Bolza [5], and also by Spallek [79]. Spallek did not give $h_6$, but instead gave an explicitly written out version of $h_4, h_{10}, h_{12}$, and

$$h_{16} = \sum_{\substack{C \in S \\ d \in C}} \theta[d]^8 \prod_{c \in T \setminus C} \theta[c]^4,$$

filling a full page, together with the formulas for $I_2, I_4, I_{10}$ of Lemma 7.3 and the formula

$$I_6(C) = h_{16}(Z)/h_{10}(Z).$$

The same page-filling formulas later appeared in [97] and [27], and, in a form that fills 'only' half a page, in [20, Section 6.3.3].

**Corollary 7.5.** Each element of the ring $\mathbf{Q}[I_2, I_4, I_6', I_{10}^{-1}]$ can be expressed as a polynomial in the theta constants divided by a power of the product of all even theta constants.

By Corollary 7.5, if we give upper and lower bounds on the absolute values of the theta constants, then we get upper bounds on the absolute values of the absolute Igusa invariants. Furthermore, we can bound the precision needed for the theta constants in terms of the precision needed for the absolute invariants.

**Remark 7.6.** Our invariants $i_1$, $i_2$, and $i_3$ are chosen to have the minimal number of factors $h_{10}$ in the denominator. Lemma 7.3 is part of the motivation for this choice. This choice is also good for the denominators, as we will see in Remark 9.3.

## 7.2 Bounds on the theta constants

For $Z \in \mathcal{H}_2$, denote the real part of $Z$ by $X$ and the imaginary part by $Y$, write $Z$ as

$$Z = \begin{pmatrix} z_1 & z_3 \\ z_3 & z_2 \end{pmatrix},$$

and let $x_j$ be the real part of $z_j$ and $y_j$ the imaginary part for $j = 1, 2, 3$. Recall that $\mathcal{B} \subset \mathcal{H}_2$ is given by

(S1) $X$ is reduced, i.e., $-1/2 \le x_i < 1/2$ for $i = 1, 2, 3$,

(S2) $Y$ is reduced, i.e., $0 \le 2y_3 \le y_1 \le y_2$, and

(B) $y_1 \ge \sqrt{3/4}$.

**Proposition 7.7.** *For every $Z \in \mathcal{B}$, we have*

$$\begin{aligned}
|\theta_j(Z) - 1| &< 0.405 && j \in \{0, 1, 2, 3\} \\
\left| \frac{\theta_j(Z)}{2E(\frac{1}{4}z_1)} - 1 \right| &< 0.348 && j \in \{4, 6\} \\
\left| \frac{\theta_j(Z)}{2E(\frac{1}{4}z_2)} - 1 \right| &< 0.348 && j \in \{8, 9\} \quad \textit{and} \\
\left| \frac{\theta_j(Z)}{2((-1)^j + E(z_3))E(\frac{1}{4}(z_1 + z_2 - 2z_3))} - 1 \right| &< 0.438 && j \in \{12, 15\}.
\end{aligned}$$

*Proof.* The proof of Proposition 9.2 of Klingen [48] gives infinite series as upper bounds for the left hand sides. A numerical inspection shows that the limits of these series are less than 0.553, 0.623, 0.623 and 0.438. Klingen's bounds can be improved by estimating more terms of the theta constants individually and thus getting a smaller error term. This has been done in Propositions 6.1 through 6.3 of Dupont [20], improving the first three bounds to 0.405, $2\,|E(z_1/2)| \le 0.514$ and $2\,|E(z_2/2)| \le 0.514$. The proof of [20, Proposition 6.2] shows that for the second and third bound, we can also take 0.348. □

**Corollary 7.8.** For every $Z \in \mathcal{B}$, we have

$$\begin{array}{rcll} |\theta_j(Z)| & < & 1.41, & (j \in \{0,1,2,3\}) \\ |\theta_j(Z)| & < & 1.37, & (j \in \{4,6,8,9\}) \\ |\theta_j(Z)| & < & 1.56. & (j \in \{12,15\}) \end{array}$$

*Proof.* These upper bounds follow immediately from (S2), (B), and Proposition 7.7. □

**Lemma 7.9.** *Let $z_3$ be a non-zero complex number with $\mathrm{Im}(z_3) \ge 0$ and $|\mathrm{Re}(z_3)| \le \frac{1}{2}$. Then we have $|1 - E(z_3)| \ge \min\{\frac{1}{4}, |z_3|\}$.*

*Proof.* If $|\mathrm{Re}(z_3)| \ge \frac{1}{6}$, then $\left|1 - e^{\pi i z_3}\right| \ge \sin(\pi/6) = \frac{1}{2}$. If $\mathrm{Im}(z_3) \ge \frac{1}{10}$, then $\left|1 - e^{\pi i z_3}\right| \ge 1 - e^{\pi/10} > \frac{1}{4}$.

If $|\mathrm{Re}(z_3)| < \frac{1}{6}$ and $\mathrm{Im}(z_3) < \frac{1}{10}$, then let $a = \pi i z_3$, so

$$\left|1 - e^{\pi i z_3}\right| = \left|a + \frac{a^2}{2!} + \frac{a^3}{3!} + \cdots\right| \ge |a|\,(1 - |a|\,(e-2)) \ge |z_3| \qquad \square$$

**Lemma 7.10.** *For every $Z \in \mathcal{B}$, we have*

$$\begin{array}{rcll} 0.59 & < & |\theta_j(Z)|\,, & (j \in \{0,1,2,3\}) \\ 1.3\ \exp(-\frac{\pi}{4}y_1) & < & |\theta_j(Z)|\,, & (j \in \{4,6\}) \\ 1.3\ \exp(-\frac{\pi}{4}y_2) & < & |\theta_j(Z)|\,, & (j \in \{8,9\}) \\ 1.05\ \exp(-\frac{\pi}{4}(y_1+y_2-2y_3)) & < & |\theta_{12}(Z)|\,, & \textit{and} \\ 1.12\ \exp(-\frac{\pi}{4}(y_1+y_2-2y_3))\nu & < & |\theta_{15}(Z)|\,, & \end{array}$$

*where $\nu = \min\{\frac{1}{4}, |z_3|\}$.*

*Proof.* This follows from Proposition 7.7 if we use Lemma 7.9 and the bounds

$$|1 + E(z_3)| > 1, \quad \exp(-\frac{\pi}{4}y_i) \ge 0.506 \quad (i \in \{1,2\}) \quad \text{and}$$

$$\exp\left(-\frac{\pi}{4}(y_1 + y_2 - 2\,|y_3|)\right) > \exp\left(-\frac{\pi}{2}y_2\right) \ge 0.256. \qquad \square$$

**Corollary 7.11.** For every $Z \in \mathcal{B}$, we have

$$\begin{aligned}
\log_2 |h_4(Z)| &< 8, \\
\log_2 |h_6(Z)| &< 13, \\
\log_2 |h_{10}(Z)| &< 11, \\
\log_2 |h_{12}(Z)| &< 17, \\
-\log_2 |h_{10}(Z)| &< \pi(y_1 + y_2 - y_3) + 3 + \max\{2, -\log_2 |z_3|\}, \\
\log_2 |i_n(Z)| &< 2\pi(y_1 + y_2 - y_3) + 64 + 2\max\{2, -\log_2 |z_3|\} \\
&\quad (n \in \{1, 2, 3\}).
\end{aligned}$$

*Proof.* The upper bounds on $h_4, h_{10}, h_{12}$, and $h_{16}$ follow from the bounds of Corollary 7.8. The lower bound on $h_{10}$ follows from the bounds of Lemma 7.10. The upper bounds on $i_n$ follow from the formulas of Lemma 7.3 and the bounds on $h_k$. □

**Remark 7.12.** Lemma 7.3, together with Corollary 7.11, gives a constructive version of (Weil's) Theorem I.6.3. Indeed, if $z_3 = 0$, then the principally polarized abelian surface $A(Z)$ corresponding to $Z$ is the product of the polarized elliptic curves $\mathbf{C}/(z_1\mathbf{Z} + \mathbf{Z})$ and $\mathbf{C}/(z_2\mathbf{Z} + \mathbf{Z})$, while if $z_3 \neq 0$, then Corollary 7.11 shows that we have $h_{10}(Z) \neq 0$, so $A(Z)$ is the Jacobian of the curve of genus 2 given by Lemma 7.3.

## 7.3 Evaluating Igusa invariants

Next, we show how to obtain approximations of absolute Igusa invariants from approximations of theta constants.

Let $z \in \mathbf{C}$ be a complex number and $n$ a non-negative integer. An *approximation* $\widetilde{z}$ of $z$ of *absolute precision* $n$ is an element of $2^{-n}\mathbf{Z}[i] \subset \mathbf{C}$. The *(absolute) error* of $\widetilde{z}$ is $\epsilon(\widetilde{z}) = |\widetilde{z} - z|$.

Let $k$ be a non-negative integer and $f : \mathbf{C}^k \to \mathbf{C}$ a map. For example, for $k = 2$, we have addition and multiplication, for $k = 0$, we have the constant $\pi$, and for $k = 1$, we have the exponential map exp, and for every fixed $m \in \mathbf{Z}$, the exponentiation $x \mapsto x^m$. For elements $z_1, \ldots, z_k \in \mathbf{C}$ with approximations $\widetilde{z}_1, \ldots, \widetilde{z}_k$, let $z = f(z_1, \ldots, z_k)$ and let $\widetilde{z}$ be $f(\widetilde{z}_1, \ldots, \widetilde{z}_k)$, rounded to a nearest element of $2^{-n}\mathbf{Z}[i]$.

For each of the examples $f$ above, the approximation $\widetilde{z}$ of $z$ can be computed from $\widetilde{z}_1, \ldots, \widetilde{z}_k$ in time

$$\widetilde{O}(n + \max\{0, \log|\widetilde{z}|, \log|\widetilde{z}_i| \quad (i = 1, \ldots, k)\})$$

using "fast multiplication" techniques (see e.g. [3]). The error $\epsilon(\widetilde{z})$ is at most

$$|z - f(\widetilde{z}_1, \ldots, \widetilde{z}_k)| + 2^{-n}.$$

Actually, the advantage of using absolute precision is that we do not have a *rounding error* in the case of addition, so that we can leave out the term $2^{-n}$ and get $\epsilon(\widetilde{z}) \le \epsilon(\widetilde{z}_1) + \epsilon(\widetilde{z}_2)$. For multiplication, we have

$$\epsilon(\widetilde{z}) \le \epsilon(\widetilde{z}_1)\,|z_2| + \epsilon(\widetilde{z}_2)\,|z_1| + \epsilon(\widetilde{z}_1)\epsilon(\widetilde{z}_2) + 2^{-n}.$$

---

**Algorithm 7.13.**
**Input:** A positive integer $s$ and approximations $\widetilde{\theta}_j(Z)$ of all even theta constants $\theta_j(Z)$ for some $Z \in \mathcal{B}$ with an absolute error of at most $2^{-s}$.
**Output:** Approximations $\widetilde{i}_n(Z)$ of the Igusa invariants $i_n(Z)$ for $n = 1, 2, 3$.

---

1. Evaluate each of the products $A$ in the definition (7.1) of the functions $h_4, h_{10}, h_{12}$, and $h_{16}$ by factor-by-factor multiplication with an absolute precision of $s$, i.e., start with $A \leftarrow 1$ and let $A \leftarrow AB$ for every factor $B$.

2. Evaluate each of the sums of in the definitions of $h_4, h_6, h_{10}$, and $h_{12}$ by term-by-term addition with an absolute precision of $s$.

3. Evaluate

$$i_1 = 2^8 h_4 h_6 h_{10}^{-1}, \quad i_2 = 2^5 h_{12} h_4^2 h_{10}^{-2}, \quad \text{and} \quad i_3 = h_4^5 h_{10}^{-2}$$

with an absolute precision of $s$.

---

**Proposition 7.14.** *Let $u = 3 + \pi(y_1 + y_2 - y_3) + \max\{2, -\log_2 |z_3|\}$. If $s$ is $> 13 + 2u$, then the output of Algorithm 7.13 has an error of at most $2^{100+3u-s}$. The running time is $\widetilde{O}(s)$ as $s$ tends to infinity, where the implied constants do not depend on the input.*

*Proof.* For any term $A$ in step 1, let $A_i$ be $A$ after $i$ factors have been multiplied together, so $|A_i| \le 1.56^i$. Let $\widetilde{A}_i$ be the approximation of $A_i$ that is computed in the algorithm, and let $\widetilde{A} = \widetilde{A}_{2k}$ be the approximation of $A$ obtained in this way. Then for the error, we have $\epsilon(\widetilde{A}_0) = 0$ and $\epsilon(\widetilde{A}_{i+1}) = 1.56\epsilon(\widetilde{A}_i) + 1.56^i 2^{-s} + 2^{-s}$. By induction, we get $\epsilon(\widetilde{A}_i) < 2^{2+i-s}$, so that the approximation $\widetilde{A}$ of each term $A$ in $h_k$ has an error of at most $\epsilon(\widetilde{A}) < 2^{2+2k-s}$. The error of $\widetilde{h}_k$ itself will therefore be less than $t_k 2^{2+2k-s} < 2^{40-s}$, where $t_4 = 10$, $t_6 = 60$, $t_{10} = 1$, and $t_{12} = 15$.

Next, we evaluate $h_{10}^{-1}$. Let $\widetilde{h}_{10}$ be the approximation that we have just computed, so $|h_{10} - \widetilde{h}_{10}| < 2^{12-s}$ and $|h_{10}| > 2^{-u}$. As we have $s > 13 + u$, we find

$$\begin{aligned} |h_{10}^{-1} - \widetilde{h}_{10}^{-1}| &= \frac{|h_{10} - \widetilde{h}_{10}|}{|h_{10}\widetilde{h}_{10}|} \\ &\leq \frac{2^{12-s}}{2^{-u}2^{-u}(1 - 2^{12-s+u})} < 2^{14+2u-s}, \end{aligned}$$

so we find an approximation of $h_{10}^{-2}$ with an error of at most $2^{14+2u-s}$.

Finally, we evaluate $i_1, i_2$, and $i_3$, and the bound on their errors follows from the absolute value and error bounds on $h_k$ and $h_{10}^{-1}$. □

## 7.4 Evaluating theta constants

The following algorithm is the naive way of evaluating theta constants, which we will use in our running time bound. Its running time is quasi-quadratic, while Dupont's (AGM-)method [20, Section 10.2] is heuristically quasi-linear. We will not prove bounds on the running time or precision of Dupont's method in this thesis.

---

**Algorithm 7.15.**
**Input:** A positive integer $s$, an approximation $\widetilde{Z}$ of a matrix $Z \in \mathcal{B}$ with sufficiently small error, and the theta characteristic $c \in \{0, \frac{1}{2}\}^{2g}$.
**Output:** An approximation $\widetilde{A}$ of $\theta[c](Z)$ with absolute error at most $2^{-s}$.

---

1. Compute
$$R = \left\lceil (0.4s + 2.2)^{1/2} \right\rceil \in \mathbf{Z}.$$

2. With an absolute precision of $t = s+1+\lfloor 2\log_2(2R+1) \rfloor$, compute an approximation $\widetilde{A}$ of
$$A = \sum_{\substack{n \in \mathbf{Z}^2 \\ |n_i| \leq R}} E\left( (n + c')Z(n + c')^t + 2(n + c')c''^t \right).$$

3. Output $\widetilde{A}$.

---

**Theorem 7.16.** *The output of Algorithm 7.15 is correct if the input is given with an absolute error of at most $2^{-t-1}$. The algorithm takes time $\widetilde{O}(s^2)$.*

*Proof.* A precision of $t$ in the input and the evaluation ensures that each term of the output approximation $\widetilde{A}$ of $A$ has an error of at most $2^{-t}$, so that we have

$$\left|A - \widetilde{A}\right| \leq (2R+1)^2 2^{-t} \leq 2^{-s-1}.$$

Next, we have

$$|A - \theta[c](Z)| \leq \sum_{\substack{n \in \mathbf{Z}^2 \\ |n_1|>R \text{ or } |n_2|>R}} \exp\left(-\frac{3\pi}{4}((n_1+c_1)^2 y_1 + (n_2+c_2)^2 y_2)\right),$$

because $0 \leq 2y_3 \leq y_1 \leq y_2$ implies $n_1^2 y_1 + n_1 n_2 y_3 + n_2^2 y_2 \geq \frac{3}{4}(n_1^2 y_1 + n_2^2 y_2)$ for all $n \in \mathbf{R}^2$. Now for positive real numbers $t$ and non-negative integers $l$, let

$$f(t,l) = \sum_{k=l}^{\infty} \exp(-\frac{3}{4}\pi k^2 t),$$

so that we find

$$|A - \theta[c](Z)| \leq 4 f(y_1, R) f(y_2, 0) + 4 f(y_1, 0) f(y_2, R),$$

If $t \geq \sqrt{3/4}$, then we have

$$f(t,l) \leq \sum_{k=l^2}^{\infty} \exp(-\frac{3}{4}\pi t k) < 1.15 \exp(-\frac{3}{4}\pi t l^2),$$

so

$$|A - \theta[c](Z)| < 5.29 \sum_{i=1}^{2} \exp(-\frac{3}{4}\pi y_i R^2) < 2^{-s-2}.$$

Therefore, we have

$$\left|\widetilde{A} - \theta[c](Z)\right| < 2^{-s-1}.$$

For each term, it takes time $\widetilde{O}(t) = \widetilde{O}(s)$ to evaluate the term and add it to the result. The number of terms is $(2R+1)^2 = \widetilde{O}(s)$, which proves the running time. □

# 8 The degree of the class polynomials

Let $K$ be a primitive quartic CM-field. In this section we give asymptotic upper and lower bounds on the degree of Igusa class polynomials of $K$. These bounds are not used in the algorithm itself, but are used in the analysis of the algorithm.

Denote the class numbers of $K$ and $K_0$ by $h$ and $h_0$ respectively, and let $h_1 = h/h_0$. The degree of the Igusa class polynomials $H_{K,n}$ for $n = 1, 2, 3$ is the number $h'$ of isomorphism classes of curves of genus 2 with CM by $\mathcal{O}_K$. By Lemma 3.5 we have $h' = h_1$ if $K$ is cyclic and $h' = 2h_1$ otherwise. The degree of the class polynomials $\widehat{H}_{K,n}$ is $h' - 1$. The following result gives an asymptotic bound on $h_1$, and hence on the degree $h'$.

**Lemma 8.1** (Louboutin [58])**.** *There exist effective constants $d > 0$ and $N$ such that for all primitive quartic CM-fields $K$ with $\Delta > N$, we have*

$$\Delta_1^{1/2}\Delta_0^{1/2}(\log \Delta)^{-d} \leq h_1 \leq \Delta_1^{1/2}\Delta_0^{1/2}(\log \Delta)^{d}.$$

*Proof.* Louboutin [58, Theorem 14] gives bounds

$$\left| \frac{\log h_1}{\log(\Delta_1\Delta_0)} - \frac{1}{2} \right| \leq d\frac{\log\log \Delta}{\log \Delta}$$

for $\Delta > N$. As we have $\Delta > \Delta_0\Delta_1$, this proves the result. □

# 9 Denominators

Let $K$ be a primitive quartic CM-field. In this section we give upper bounds on the denominators of the Igusa class polynomials of $K$. By the *denominator* of a polynomial $f \in \mathbf{Q}[X]$, we mean the smallest positive integer $c$ such that $cf$ is in $\mathbf{Z}[X]$.

A prime $p$ occurs in the denominator of $H_1$ if and only if there is a curve $C$ with CM by $\mathcal{O}_K$ such that $C$ has *stable bad reduction* at a prime $\mathfrak{p}$ over $p$. It is known that abelian varieties with complex multiplication have potential *good* reduction at all primes, but this doesn't imply that Jacobians reduce as Jacobians: the reduction of the Jacobian of a smooth curve $C$ of genus two can be a polarized product of elliptic curves $E_1 \times E_2$. The stable reduction of $C$ is then the union of those elliptic curves intersecting transversely. For details, we refer to Goren and Lauter [35, 36], who study this phenomenon and use the embedding

$$\mathcal{O}_K \to \mathrm{End}(E_1 \times E_2)$$

to bound both $p$ and the valuation of the denominator of $H_1$ at $p$.

We will first give the bounds of Goren and Lauter [35, 36] which hold in general, but are expected to be far from asymptotically optimal. These are the only bounds that we will use in our running time analysis. Then we give optimal bounds conjectured by Bruinier and Yang [8] for special cases and proven by Yang [98] in cases that are even more special. We end this section by giving a counterexample to a bound conjectured by Lauter [54].

## 9.1 The bounds of Goren and Lauter

The bounds of Goren and Lauter are given in terms of integers $a, b, d$ such that $K$ is given by $K = \mathbf{Q}(\sqrt{-a+b\sqrt{d}})$. For $d$, one can take the discriminant $d = \Delta_0$ of the real quadratic subfield $K_0$. We will prove in Lemma 9.9 below that one can take $a < 8\pi^{-1}(\Delta_1\Delta_0)^{1/2}$, where $\Delta_1 = N_{K_0/\mathbf{Q}}(\Delta_{K/K_0})$ is the norm of the relative discriminant. The denominator itself does not depend on the choice of $a$, so we can replace $a$ by this bound on $a$ in all denominator bounds below.

The main result of this section is the following.

**Theorem 9.1.** *Let $K$ be a primitive quartic CM-field and write*

$$K = \mathbf{Q}\Big(\sqrt{-a+b\sqrt{d}}\Big) \quad \textit{with} \quad a, b, d \in \mathbf{Z}.$$

*The denominator of each of the Igusa class polynomials of $K$ divides $2^{14h'}D^2$ for*

$$D = \left( \prod_{\substack{p<4da^2 \\ p \text{ prime}}} p^{\lfloor 4f(p)(1+\log(2da^2)/\log p)\rfloor} \right)^{h'},$$

*where $f(p)$ is given by $f(p) = 8$ if $p$ ramifies in $K/\mathbf{Q}$ and satisfies $p \le 3$, and given by $f(p) = 1$ otherwise.*

*Furthermore, the result above remains true if we replace $d$ by $\Delta_0$ and $a$ by $\lfloor 8\pi^{-1}(\Delta_1\Delta_0)^{1/2}\rfloor$ in the definition of $D$. We then have $\log D = \widetilde{O}(h'\Delta) = \widetilde{O}(\Delta_1^{3/2}\Delta_0^{5/2})$ as $\Delta$ tends to infinity.*

We will prove this result below.

**Remark 9.2.** Theorem 9.1 as stated holds for the absolute Igusa invariants $i_1$, $i_2$, $i_3$ of Section 2. For another choice of a set $S$ of absolute Igusa invariants, take positive integers $c_3$ and $k$ such that $c_3(2^{-12}I_{10})^k S$ consists of modular forms of degree $k$ with integral Fourier expansion.

Then the denominator divides $c_3^{h'} D^k$. See the proof of Theorem 9.1 below for details.

Using the formulas for the Igusa invariants of Lemma 7.3, one can verify that all elements of $\mathbf{Z}[2^{-15} I_2 I_{10}, 2^{-2} I_4, 2^{-2} I'_6, 2^{-12} I_{10}]$ have an integral Fourier expansion. For this Fourier coefficient computation, see Appendix 1. For our invariants, we have $c_3 = 2^{14}$ and $k = 2$.

**Remark 9.3.** Our invariants $i_1$, $i_2$, and $i_3$ are chosen to have the minimal value for $k$. Remark 9.2 is part of the motivation for this choice. This choice is also good for getting small absolute values of the coefficients, as we have seen in Remark 7.6. We have $k = 1$ for $i_1$ and $k = 2$ for $i_2$ and $i_3$.

We did not normalize our invariants with powers of 2 to get $c_3 = 1$, because invariants without these powers of 2 are easier to remember and yield smaller class polynomials in practice.

**Remark 9.4.** It follows from Goren [34, Thms. 1 and 2] that Theorem 9.1 remains true if one restricts in the product defining $D$ to primes $p$ that divide $2 \cdot 3 \cdot c_3 \Delta$ or factor as a product of two prime ideals in $\mathcal{O}_K$. See also Goren and Lauter [36, Tables 3.3.1 and 3.5.1].

The first part of the proof of Theorem 9.1 is the following bound on the primes that occur in the denominator.

**Lemma 9.5** (Goren and Lauter [35])**.** *The coefficients of each of the polynomials $H_{K,n}(X)$ and $\widehat{H}_{K,n}$ for $K = \mathbf{Q}(\sqrt{-a + b\sqrt{d}})$ a primitive quartic CM-field are $S$-integers, where $S$ is the set of primes smaller than $4da^2$.*

*Proof.* Corollary 5.2.1 of [35] is this result with $4d^2a^2$ instead of $4da^2$. We can however adapt the proof as follows to remove a factor $d$. In [35, Corollary 2.1.2], it suffices to have only $N(k_1)N(k_2) < p/4$ in order for two elements $k_1$ and $k_2$ of the quaternion order ramified in $p$ and infinity to commute. Then, in the proof of [35, Theorem 3.0.4], it suffices to take as hypothesis only $p > d(\mathrm{Tr}(r))^2$. As we have $d(\mathrm{Tr}(r))^2 \geq d\delta_1\delta_2 \geq N(x)N(by^\vee)$, this implies that $x$ and $by^\vee$ are in the same imaginary quadratic field $K_1$. As in the original proof, this implies that $ywy^\vee$ is also contained in $K_1$ and hence $\psi(\sqrt{r}) \in M_2(K_1)$, so there is a morphism $K = \mathbf{Q}(\sqrt{r}) \mapsto M_2(K_1)$, contradicting primitivity of $K$. □

**Remark 9.6.** Lemma 9.5 as phrased above is for class polynomials defined in terms of the invariants $i_1$, $i_2$, $i_3$ of Section 2. If other invariants are used, then the result is still valid if the primes dividing $c_3$ of Remark 9.2 are added to $S$.

Recent results of Eyal Goren bound the exponents to which primes may occur in the denominator as follows.

**Lemma 9.7** (Goren-Lauter [36])**.** *Let $K$ be a primitive quartic CM-field and $C/\mathbf{C}$ a curve of genus 2 that has CM by $\mathcal{O}_K$. Let $v$ be a non-archimedean valuation of $L(i_n(C))$, normalized with respect to $\mathbf{Q}$ in the sense that $v(\mathbf{Q}^*) = \mathbf{Z}$ holds, and let $e$ be its ramification index (so $ev$ is normalized with respect to $L(i_n(C))$. Let $k$ and $c_3$ be as in Remark 9.2.*

*Then we have*

$$-v(i_n(C)) \le 4k(\log(2da^2)/\log(p) + 1) + v(c_3) \qquad \text{if } e \le p-1, \text{ and}$$
$$-v(i_n(C)) \le 4k(8\log(2da^2)/\log(p) + 2) + v(c_3) \qquad \text{otherwise.} \tag{9.8}$$

*Moreover, $e \le p-1$ is automatic for $p \ne 2, 3$.*

*Proof.* Theorem 7.0.4 of Goren and Lauter [36] gives the valuation bounds.

Next, we show $e \le 4$ for $p > 2$. Let $L \subset \mathbf{C}$ be isomorphic to the normal closure of $K$, let $\Phi$ be the CM-type of $C$ and $K^{\mathrm{r}} \subset L$ its reflex field. The extension $K^{\mathrm{r}}(i_n(C))/K^{\mathrm{r}}$ is unramified by the main theorem of complex multiplication I.9.1. In particular, the ramification index of any prime in $L(i_n(C))/\mathbf{Q}$ is at most its ramification index in $L/\mathbf{Q}$. By Lemma I.3.4, the field $L$ has degree 4 over $\mathbf{Q}$ or has degree 2 over a biquadratic subfield, hence we have $e \le 4$ for $p > 2$. □

Lemma's 9.5 and 9.7 hold for any representation of $K$ of the form $K = \mathbf{Q}(\sqrt{-a + b\sqrt{d}})$, hence in particular for such a representation with $da^2$ minimal. The following result gives a lower and an upper bound on the minimal $da^2$.

**Lemma 9.9.** *Let $K$ be a quartic CM-field with discriminant $\Delta$ and let $\Delta_0$ be the discriminant of the real quadratic subfield $K_0$.*

*For all $a, b, d \in \mathbf{Z}$ such that $K = \mathbf{Q}(\sqrt{-a + b\sqrt{d}})$ holds, we have $a^2 > \Delta_1$ and $d \ge \frac{1}{4}\Delta_0$. Conversely, there exist such $a, b, d \in \mathbf{Z}$ with $d = \Delta_0$ and $a^2 < (\frac{8}{\pi})^2 \Delta_1 \Delta_0$.*

*Proof.* The lower bounds are trivial, because $\Delta_0$ divides $4d$ and $\Delta_1$ divides $a^2 - b^2 d \le a^2$. For the upper bound, we show the existence of a suitable element $-a + b\sqrt{\Delta_0}$ using a geometry of numbers argument.

We identify $K \otimes_{\mathbf{Q}} \mathbf{R}$ with $\mathbf{C}^2$ via its pair of infinite primes. Then $\mathcal{O}_K$ is a lattice in $\mathbf{C}^2$ of covolume $2^{-2}\sqrt{\Delta}$. Let $\omega_1, \omega_2$ be a $\mathbf{Z}$-basis of $\mathcal{O}_{K_0}$, and consider the open parallelogram $\omega_1(-1,1) + \omega_2(-1,1) \subset \mathcal{O}_{K_0} \otimes \mathbf{R} \cong \mathbf{R}^2$. We define the open convex symmetric region

$$V_Y = \{x \in \mathbf{C}^2 : \mathrm{Re}(x) \in \omega_1(-1,1) + \omega_2(-1,1), (\mathrm{Im}\, x_1)^2 + (\mathrm{Im}\, x_2)^2 < Y\}.$$

Then $\mathrm{vol}(V_Y) = 4\pi\sqrt{\Delta_0}Y$ and by Minkowski's convex body theorem, $V_Y$ contains a non-zero element $\alpha \in \mathcal{O}_K$ if we have

$$\mathrm{vol}(V_Y) > 2^4 \operatorname{covol} \mathcal{O}_K = 4\sqrt{\Delta}.$$

We pick $Y = \sqrt{\Delta_1\Delta_0}\pi^{-1} + \epsilon$, so that $\alpha$ exists.

Let $r = 4(\alpha - \overline{\alpha})^2$, which is of the form $-a + b\sqrt{\Delta_0}$ with integers $a$ and $b$. Now $a = \frac{1}{2}|r_1 + r_2| = 2(2\operatorname{Im} x_1)^2 + 2(2\operatorname{Im} x_2)^2 < 8Y = 8\sqrt{\Delta_1\Delta_0}\pi^{-1} + 8\epsilon$. As $a$ is in the discrete set $\mathbf{Z}$, and we can take $\epsilon$ arbitrarily close to 0, we find that we can even get $a \leq 8\sqrt{\Delta_1\Delta_0}\pi^{-1}$ and hence $a^2 \leq (\frac{8}{\pi})^2\Delta_1\Delta_0$. □

*Proof of Theorem 9.1.* Lemma 9.5 proves that the denominator of the Igusa class polynomials is divisible only by primes dividing $D$.

Next, let $v$ be any normalized non-archimedean valuation of $H_{K^{\mathrm{r}}}$ and $c$ any coefficient of $H_{K,n}$ or $\widehat{H}_{K,n}$. Then $c$ is a sum of products, where each product consists of at most $h'$ factors $i_n(C)$ for certain $n$'s and $C$'s. This shows that $-v(c)$ is at most $h'$ times the right hand side of (9.8), hence $v(Dc) \geq 0$. As this holds for all $v$, it follows that $Dc$ is an integer. This concludes the proof that $DH_{K,n}$ and $D\widehat{H}_{K,n}$ are in $\mathbf{Z}[X]$.

The fact that we can replace $a$ and $d$ as in the theorem is Lemma 9.9. Next, we prove the asymptotic bound on $D$. Note that the exponent of every prime in $D^{1/h'}$ is linear in $\log\Delta$, as is the bit size of every prime divisor of $D$. Therefore, $\log D$ is $\widetilde{O}(h'N)$, where $N = O(\Delta)$ is the number of prime divisors of $D$, which finishes the proof of Theorem 9.1. □

## 9.2 The bounds of Bruinier and Yang

In this section, we give an improvement of the bounds in Theorem 9.1, which is proven only for a small subset of the set of CM-fields. The denominator bound in this section is not directly relevant to our main theorem, but is interesting as it is optimal.

Let $K_0^{\mathrm{r}}$ be the real quadratic subfield of the reflex field $K^{\mathrm{r}}$ of $K$ (as defined e.g. in the proof of Lemma 9.7). Then we have $K_0^{\mathrm{r}} = \mathbf{Q}(\sqrt{\Delta_1})$.

**Theorem 9.10** (Yang [98])**.** *Let $K$ be a primitive quartic CM-field such that $\Delta_0$ and $\Delta_1$ are prime and $\mathcal{O}_K$ is monogenic over $\mathcal{O}_{K_0}$, i.e., of the form $\mathcal{O}_K = \mathcal{O}_{K_0}[\alpha]$ for some $\alpha \in K$. Let $k$ and $c_3$ be as in Remark 9.2.*

*For any fractional $\mathcal{O}_{K_0}$-ideal $\mathfrak{a}$, let*

$$\rho(\mathfrak{a}) = \#\{\mathfrak{A} \subset \mathcal{O}_{K^{\mathrm{r}}} \mid N_{K^{\mathrm{r}}/K_0^{\mathrm{r}}}\mathfrak{A} = \mathfrak{a}\}.$$

*Let $\mathfrak{d} \subset \mathcal{O}_{K_0^{\mathrm{r}}}$ be the relative discriminant of $K^{\mathrm{r}}/K_0^{\mathrm{r}}$, and for any $t \in \mathfrak{d}^{-1}$, let*

$$C_t = \prod_{\substack{\mathfrak{p} \subset \mathcal{O}_{K_0^{\mathrm{r}}} \\ \mathfrak{p} \text{ prime}}} N_{K_0^{\mathrm{r}}/\mathbf{Q}}(\mathfrak{p})^{(\mathrm{ord}_{\mathfrak{p}}(t)+1)\rho(t\mathfrak{d}\mathfrak{p}^{-1})} \quad \in \mathbf{Z}.$$

*Let $S$ be the set of pairs $(n, \ell) \in \mathbf{Z}^2$ such that $n$ is positive, odd, and less than $\sqrt{\Delta_0}$, that $\ell$ satisfies $4\,|\ell| < (\Delta_0 - n^2)\sqrt{\Delta_1}$, and that*

$$t(\ell, n) = (4\ell + (\Delta_0 - n^2)\sqrt{\Delta_1})/(8\Delta_0) \in K_0^{\mathrm{r}}$$

*is an element of $\mathfrak{d}^{-1}$.*

*Then the denominator of the constant coefficient of each Igusa class polynomial $H_{K,n}$ of $K$ divides*

$$D' = c_3^{h'} \prod_{(n,\ell) \in S} C_{t(\ell,n)}^k.$$

*Proof.* Note first that $D'$ is indeed finite, because $\rho(t\mathfrak{d}\mathfrak{p}^{-1})$ is zero unless $\mathfrak{p}$ divides the integral ideal $t\mathfrak{d}$.

As $\mathcal{O}_K$ is monogenic over $\mathcal{O}_{K_0}$, the relative discriminant of $K/K_0$ is a square modulo 4, hence the same holds for its norm $\Delta_1$. As $\Delta_1$ is prime, this implies that it is 1 modulo 4, and that the discriminant of $K_0^{\mathrm{r}} = \mathbf{Q}(\sqrt{\Delta_1})$ is equal to $\Delta_1$.

Under the conditions that we just checked, Theorem 9.1 of [98] states exactly $D' H_{K,n} \in \mathbf{Z}[X]$, except that it does so

- only for Spallek's absolute invariants
- under the assumption that $K$ has only two roots of unity.

The proof applies to all absolute invariants. If, furthermore, $K$ is not isomorphic to $\mathbf{Q}(\zeta_5)$, then its number of roots of unity is indeed 2. This proves the result for $K \ncong \mathbf{Q}(\zeta_5)$.

For $K = \mathbf{Q}(\zeta_5)$, we have seen in Example I.6.1 that the Jacobian $J(C)$ of $C : y^2 = x^5 + 1$ has CM by $\mathcal{O}_K$. By Lemma 3.5, this is the only principally polarized abelian surface with CM by $\mathcal{O}_K$. The Igusa invariants $I_2$, $I_4$, and $I_6$ of this curve are zero, which proves the result also for $K = \mathbf{Q}(\zeta_5)$. □

**Remark 9.11.** Theorem 9.10 is stated only for the constant coefficient of the class polynomials $H_{K,n}$. The bound comes from an arithmetic intersection number of cycles. From the fact that the relevant cycles are effective and intersect properly ([98]), it should be straightforward to derive that the bound holds for all coefficients of $H_{K,n}$ and in fact even for $\widehat{H}_{K,n}$.

**Remark 9.12.** The denominator bound $D'$ is sharp in the sense that (by [98, Corollary 1.6]) the set of primes dividing $D'$ are exactly the primes $p$ such that there exists a curve with CM by $\mathcal{O}_K$ of stable bad reduction at a prime over $p$.

**Remark 9.13.** If Bruinier and Yang's conjecture ([8, equation (1.10)], [98, Conjecture 1.1]) is true, then Theorem 9.10 holds in slightly greater generality.

### 9.3 Counterexample to a conjectured formula

A conjecture of Lauter [54] also bounds the primes dividing the denominators of Igusa class polynomials by stating that each such prime divides $\Delta - x^2$ for some non-negative integer $x < \Delta^{1/2}$. However, the field $K = \mathbf{Q}[X]/(X^4 + 558X^2 + 31873)$ with $\Delta_0 = 17$ and $\Delta_1 = 31873$ is a counterexample, as demonstrated by the corresponding entry in the ECHIDNA database [50]. The prime 7499 divides the denominators of the class polynomials, but does not divide $\Delta - x^2$ for any small enough $x$. The conjecture did not go down without a fight: our search of the database reveiled only 17 counterexamples among thousands of CM-fields, and we know no counterexamples with class number $h \leq 14$.

## 10 Recovering a polynomial from its roots

In this section, we show how to compute a polynomial from complex approximations of its roots. This will tell us the precision to which we need to know these roots. The algorithms in this section are well known to the experts, but we did not find an error analysis in the literature.

We will compute an approximation of a polynomial from approximations of its roots in Sections 10.1 and 10.2. Then in Section 10.3, we compute numerators and denominators of the coefficients from their approximations.

### 10.1 Polynomial multiplication

For a complex polynomial $g$, let $|g|_1$ (resp. $|g|_\infty$) be the sum (resp. maximum) of the absolute values of the coefficients of $g$. We find $|g_1 g_2|_\infty \leq |g_1|_\infty |g_2|_1$ and $|g|_1 \leq (\deg(g) + 1)\,|g|_\infty$.

The following algorithm computes products of *integer* polynomials.

---

**Algorithm 10.1.**
**Input:** Polynomials $g_1, g_2 \in \mathbf{Z}[X]$, given by the binary expansions of their coefficients.
**Output:** The product $g_1 g_2 \in \mathbf{Z}[X]$.

---

1. Let $k = \lceil \log_2 |g_1|_\infty \rceil + \lceil \log_2 |g_2|_\infty \rceil + \lceil \log_2(\deg(g_1) + 1) \rceil$.
2. Evaluate the polynomials at $2^k$ by writing the binary expansions of their coefficients after each other with the appropriate number of zeroes between them.
3. Multiply the results of step 2 using fast integer multiplication.
4. Read off the binary expansions of the coefficients of $g_1 g_2$ from the result of step 3.

---

This algorithm has a running time of $M((\deg(g_1 g_2)+1) \log_2 |g_1 g_2|_\infty)$, where $M(n) = O(n \log n \log\log n)$ is the time needed for a multiplication of $n$-bit integers. See also [90, Corollary 8.27].

For a complex polynomial $g \in \mathbf{C}[X]$ and a positive integer $p$, an *approximation* $\widetilde{g}$ of $g$ with *absolute precision* $p$ is an object of the form $2^{-p}(a + ib)$, where $a$ and $b$ are polynomials in $\mathbf{Z}[x]$ given by the binary expansions of their coefficients. Complex numbers are complex polynomials of degree 0 and have approximations as such, which is exactly the notion of approximation from Section 7.3. The *error* of an approximation $\widetilde{g}$ of a polynomial $g$ is $\epsilon(\widetilde{g}) = |g - \widetilde{g}|_\infty$. Suppose we have approximations $\widetilde{g}_k = 2^{-p}(a_k + ib_k)$ of $g_k$ for $k = 1, 2$ with absolute precision $p$. The following algorithm computes an approximation $\widetilde{g_1 g_2}$ of the product $g_1 g_2$ with the same absolute precision. It does so by computing the product $\widetilde{g}_1 \widetilde{g}_2$ exactly, and then reducing the precision back to $p$.

---

**Algorithm 10.2.**
**Input:** Approximations $\widetilde{g}_1 = 2^{-p}(a_1 + ib_1)$ and $\widetilde{g}_2 = 2^{-p}(a_2 + ib_2)$ of complex polynomials $g_1, g_2$.
**Output:** An approximation $\widetilde{g_1 g_2} = 2^{-p}(a + ib)$ of $g_1 g_2$.

---

1. Compute $a' = a_1 a_2 - b_1 b_2$ and $b' = a_1 b_2 + b_1 a_2$ in $\mathbf{Z}[X]$ using Algorithm 10.1.

2. Let $a \in \mathbf{Z}[X]$ be obtained from $a'/2^p \in \mathbf{Q}[X]$ by rounding each coefficient to the nearest integer. Let $b \in \mathbf{Z}[X]$ be obtained from $b'/2^p$ in the same way.

---

**Lemma 10.3.** *Algorithm 10.2 takes time*

$$M((\deg(g_1 g_2) + 1)(\log_2 |g_1 g_2|_\infty + 2^p)).$$

*The error* $\epsilon(\widetilde{g_1 g_2})$ *is at most*

$$|g_1|_1 \, \epsilon(\widetilde{g}_2) + |g_2|_1 \, \epsilon(\widetilde{g}_1) + (\deg(g_1) + 1)\epsilon(\widetilde{g}_1)\epsilon(\widetilde{g}_2) + 2^{-p}.$$

*Proof.* The running time bound follows from the fact that we simply apply Algorithm 10.1 four times. The triangle inequality for $|\cdot|_\infty$ gives us the bound on the error. □

## 10.2 Recovering a polynomial from its roots

Let $z_1, \ldots, z_n$ be complex numbers. The purpose of this section is to compute an approximation of $f = \prod_{i=1}^n (X - z_i) \in \mathbf{C}[X]$ from an approximation of $z_1, \ldots, z_n$. Suppose that we know $s_i \in \mathbf{Q}$ satisfying $|z_i| + 1 \leq s_i$ for $i = 1, \ldots, n$, and let $s = \prod s_i$.

---

**Algorithm 10.4.**
**Input:** an integer $u > 0$ and approximations $\widetilde{z}_1, \ldots, \widetilde{z}_n$ of $z_1, \ldots, z_n$ with error

$$\epsilon(\widetilde{z}_i) \leq 2^{-u - \sum_{j \neq i} \log_2 s_j - 3\log_2 n - 3}.$$

**Output:** an approximation $\widetilde{f}$ of $f = \prod_{i=1}^n (X - z_i) \in \mathbf{C}[X]$ with error $\epsilon(\widetilde{f}) \leq 2^{-u}$.

---

1. Build a binary tree of depth $l = \lceil \log_2 n \rceil$ with at $n$ of the leaves the $n$ linear polynomials $X - \widetilde{z}_i$, and at the remaining $2^l - n$ leaves the constant polynomial 1.

2. From the leaves up to the root, at every node $t$ of the tree, put the product $\widetilde{g}_t$ of the two nodes below it, computed by Algorithm 10.2 with absolute precision $p = u + \sum_j \log_2 s_j + 3\log_2 n + 3$, where the sum is taken over those $j$ that are not below the node $t$.

3. Output the root of the tree.

---

**Theorem 10.5.** *Algorithm 10.4 is correct and has a running time of*

$$O(nm\log(nm)^2\log\log(nm)),$$

*where* $m = \max\{u, \log n, \log s\}$.

*Proof of Theorem 10.5.* For every node $t$ of the tree, denote by $d(t)$ the set of leaves $i$ below $t$. For every node $t$ of the tree, let $g_t$ be the polynomial

$$g_t = \prod_{i\in d(t)} (X - z_i)$$

of which the polynomial $\widetilde{g}_t$ computed in the algorithm is an approximation. Let $b_k$ be the maximum over all nodes $t$ at distance at most $k$ to the leaves of

$$|g_t|_1 \prod_{i\in d(t)} s_i^{-1}.$$

Similarly, let $\kappa_k$ be the maximum over all nodes $t$ at distance at most $k$ to the leaves of

$$\max\{2^{-p}, \epsilon(\widetilde{g}_t) \prod_{i\in d(t)} s_i^{-1}\}.$$

Then $b_k \le 1$ for all $k$. Therefore, by Lemma 10.3, we have

$$\kappa_{k+1} \le 2\kappa_k + (2^k+1)\kappa_k^2 + 2^{-p} \le 3\kappa_k + (2^k+1)\kappa_k^2.$$

If $\kappa_0 \le n^{-3}$, then by induction this implies that $\kappa_k \le 4^k\kappa_0$ for all $k$, so $\kappa_l < (2n)^2\kappa_0$. In particular, the error of each coefficient of the output is at most $(2n)^2\kappa_0 s$.

This means that $\kappa_0 = 2^{-u-3\log n-3-\log_2 s}$ is sufficient. At the $k$-th level of the tree, there are $2^{l-k}$ polynomial multiplications of degree at most $2^k$ where each coefficient has a bit size of $O(m)$, so each of the $l < 1+\log_2 n$ levels takes time $O(M(nm))$, which proves the complexity. □

**Remark 10.6.** Algorithm 10.4 is Algorithm 10.3 of [90], except that we round the coefficients back to a fixed precision after every polynomial multiplication. A direct application of the algorithm in [90] would yield exactly the product

$$\prod_{k=1}^{n}(X - \widetilde{z}_k)$$

with a very large denominator in time that is quasi-quadratic rather than quasi-linear.

## 10.3 Recognizing rational coefficients

There are various ways of recognizing a polynomial $f \in \mathbf{Q}[X]$ from an approximation $\widetilde{f}$. If one knows an integer $D$ such that the denominator of $f$ divides $D$, and the error $\epsilon(\widetilde{f})$ is less than $(2D)^{-1}$, then $Df$ is obtained from $D\widetilde{f}$ by rounding the coefficients to the nearest integers.

Other methods to compute $f$ from $\widetilde{f}$ are based on continued fractions, where the coefficients of $f$ are obtained via the continued fraction expansion of the coefficients of $\widetilde{f}$, or on the LLL-algorithm, where the coefficients of an integral multiple of $f$ arise as coordinates of a small vector in a lattice [57, Section 7]. Such methods have the advantage that only a bound $B$ on the denominator needs to be known, instead of an actual multiple $D$. This is very useful in practical implementations, because one can guess a small value for $B$, which may be much smaller than any proven $D$. In the case of Igusa class polynomials, there exist a few good heuristic checks of the output when using a non-proven bound $B$, such as smoothness of the denominators, and successfulness of explicit CM constructions.

For our purpose of giving a proven running time bound however, we prefer the first method of rounding $D\widetilde{f}$, since it is easy to analyze and asymptotically fast. The following algorithm computes $D$ for the case of Igusa class polynomials.

---

**Algorithm 10.7.**
**Input**: The discriminant $\Delta$ of a primitive quartic CM-field $K$ and the degree $h'$ of the Igusa class polynomials of $K$.
**Output**: The integer $D$ of Theorem 9.1, which satisfies $DH_{K,n} \in \mathbf{Z}[X]$ for $n = 1, 2, 3$.

---

1. List all primes up to the number $4da^2$ as in Theorem 9.1.
2. Raise each prime in the list to the exponent in Theorem 9.1.
3. Compute the product of the integers of step 2 using a binary tree, just as we used a binary tree to compute a product of polynomials in Algorithm 10.4. See also [90, Exercise 10.8].

---

Algorithm 10.7 takes time $\widetilde{O}(\log D)$, so we conclude that we can compute $H_{K,n}$ from an approximation $\widetilde{H_{K,n}}$ in time $\widetilde{O}(\log D)$ plus time linear in the bit size of $\widetilde{H_{K,n}}$, provided that we have $\epsilon(\widetilde{H_{K,n}}) < (2D)^{-1}$.

# 11 The algorithm

---

**Algorithm 11.1.**
**Input:** A positive quadratic fundamental discriminant $\Delta_0$ and positive integers $a$ and $b$ such that the the field

$$K = \mathbf{Q}(\sqrt{-a + b\sqrt{\Delta_0}})$$

is a primitive quartic CM-field of discriminant greater than $a$.
**Output:** The Igusa class polynomials $H_{K,n}$ for $n = 1, 2, 3$.

---

1. Compute a $\mathbf{Z}$-basis of $\mathcal{O}_K$ using the algorithm of Buchmann and Lenstra [9] and use this to compute the discriminant $\Delta$ of $K$.

2. Compute a complete set $\{A_1, \ldots, A_{h'}\}$ of representatives of the $h'$ isomorphism classes of principally polarized abelian surfaces over $\mathbf{C}$ with CM by $\mathcal{O}_K$, using Algorithm 3.1. Here each $A_j$ is given by a triple $(\Phi_j, \mathfrak{a}_j, \xi_j)$ as in Section 3.3.

3. From $\Delta$ and $h'$, compute a number $D$ such that $DH_{K,n}$ is in $\mathbf{Z}[X]$ for $n = 1, 2, 3$, using Algorithm 10.7.

4. For $j = 1, \ldots, h'$, do the following.

   (a) Compute a symplectic basis of $\mathfrak{a}_j$ using Algorithm 4.2. This provides us with a period matrix $W_j \in \mathcal{H}_2 \cap \mathrm{Mat}_2(L)$, where $L \subset \mathbf{C}$ is the normal closure of $K$.

   (b) Replace the period matrix $W_j$ by an $\mathrm{Sp}_4(\mathbf{Z})$-equivalent period matrix $Z_j \in \mathcal{F}_2 \cap \mathrm{Mat}_2(L)$, using Algorithm 5.9.

   (c) Let $u_j = \lceil 3 + (y_1 + y_2 - y_3)\pi + \max\{2, -\log_2 |z_3|\} \rceil$, where

$$Z_j = \begin{pmatrix} z_1 & z_3 \\ z_3 & z_2 \end{pmatrix} \quad \text{and} \quad y_k = \operatorname{Im} z_k \quad (k = 1, 2, 3).$$

5. Let $p = \lceil \log_2 D + 3 \log_2 h' + 4 \rceil + \sum_{j=1}^{h'} (2u_j + 40)$. This is the precision with which we will approximate the Igusa invariants.

6. For $j = 1, \ldots, h'$, do the following.

   (a) Evaluate the theta constants in $Z_j$, using Algorithm 7.15, to a precision $r_j = 101 + 7u_j + p$.

(b) Use Algorithm 7.13 to evaluate $i_n(A_j)$ for $(n = 1, 2, 3)$ to precision $p$.

7. For $n = 1, 2, 3$, do the following.

   (a) Use Algorithm 10.4 to compute an approximation $\widetilde{H}_{K,n}$ of $H_{K,n}$ for $n = 1, 2, 3$ from the approximations of Igusa invariants of step 6b.

   (b) Compute $DH_{K,n}$ by rounding the coefficients of $D\widetilde{H}_{K,n}$ to nearest integers.

   (c) Output $H_{K,n}$.

The polynomials $\widehat{H}_{K,n}$ $(n = 2, 3)$ of Section 2.2 can be computed from the approximations of $i_n(C)$ and $i_1(C)$ efficiently using Algorithm 10.9 of [90] (see also [23, Section 4]). However, instead of doing a detailed rounding error analysis of that algorithm, we give a more naive and slower algorithm that is still much faster than the running time in our Main Theorem. To compute the polynomials $\widehat{H}_{K,n}$, we simply modify step 7a as follows:

1. Evaluate each summand in the definition of the polynomial $\widehat{H}_{K,n}$ using Algorithm 10.4.

2. Evaluate $\widetilde{H}_{K,n}$ using a binary tree as in Algorithm 10.4 with addition instead of multiplication.

---

We now recall and prove the main theorem.

**Main Theorem.** *Algorithm 11.1 computes $H_{K,n}$ $(n = 1, 2, 3)$ for any primitive quartic CM-field $K$. It has a running time of $\widetilde{O}(\Delta_1^{7/2}\Delta_0^{11/2})$ and the bit size of the output is $\widetilde{O}(\Delta_1^2\Delta_0^3)$.*

*Proof.* We start by proving that the output is correct. By Proposition 7.14, the precision $r_j$ for the theta constants suffices to get the absolute Igusa invariants with precision $p$. Corollary 7.11 tells us that we have $|i_n(Z_j)| \leq 2^{6u_j+77}$. These bounds and Theorem 10.5 show that it suffices to know the absolute Igusa invariants to precision $p$ in order to get a precision of $1 + \log_2 D$ bits for the coefficients of $H_{K,n}$. By Theorem 9.1, the polynomials $DH_{K,n}$ have integer coefficients, so a precision of $1 + \log_2 D$ for the coefficients of $H_{K,n}$ suffices for recognizing these coefficients and getting a correct output. This proves that the output of Algorithm 11.1 is correct.

Next, we bound the precisions $p$ and $r_j$. We start by bounding $u_j$, for which we need an upper bound on $y_1 + y_2 - y_3$ and a lower bound on $z_3$. We have $y_2 \geq y_1$ and $y_3 \geq 0$, hence $y_1 + y_2 - y_3 \leq 2y_2$, and Corollary 6.2 gives the upper bound

$$y_2 \leq \max\{\frac{2\sqrt{2}}{\sqrt{3}\pi}\Delta_0, \frac{4}{9}\Delta_1^{1/4}\Delta_0^{1/2}\}.$$

We claim that the off-diagonal entry $z_3$ of $Z_j \in \mathcal{H}_2$ is non-zero. Indeed, if $z_3 = 0$, then $Z_j = \mathrm{diag}(z_1, z_2)$ with $z_1, z_2 \in \mathcal{H} = \mathcal{H}_1$ and $A_j$ is the product of the elliptic curves corresponding to $z_1$ and $z_2$, contradicting the fact that $A_j$ is simple (Theorem I5.2). The claim and Corollary 5.19 together now give an upper bound on $\log(1/z_3)$, which is polynomial in $\log \Delta$ by Lemma 3.6.

We now have

$$u_j = O(\max\{\frac{2\sqrt{2}}{\sqrt{3}\pi}\Delta_0, \frac{4}{9}\Delta_1^{1/4}\Delta_0^{1/2}\}),$$

$h' = \widetilde{O}(\Delta_1^{1/2}\Delta_0^{1/2})$, and by Theorem 9.1 also $\log D = \widetilde{O}(\Delta_1^{3/2}\Delta_0^{5/2})$. We find that $p$ is dominated by our bounds on $\log D$, hence we have $p = \widetilde{O}(\Delta_1^{3/2}\Delta_0^{5/2})$ and also $r_j = \widetilde{O}(\Delta_1^{3/2}\Delta_0^{5/2})$.

Finally, we can bound the running time. Under the assumption that $K$ is given as $K = \mathbf{Q}(\sqrt{-a + b\sqrt{\Delta_0}})$, where $\Delta_0$ is a positive fundamental discriminant and $a, b$ are positive integers such that $a < \Delta_0$, we can factor $(a^2 - b^2\Delta_0)\Delta_0^2$ and hence find the ring of integers in step 1 in time $O(\Delta)$.

As shown in Section 3.3, step 2 takes time $\widetilde{O}(\Delta^{1/2})$. Step 3 takes time $\widetilde{O}(D) = \widetilde{O}(\Delta_1^{3/2}\Delta_0^{5/2})$.

For every $j$, step 4a takes time polynomial in $\log \Delta$ by Lemma 3.6 and Theorem 5.18. The same holds for steps 4b and 4c and each summand of step 5. The number of iterations or summands of these steps is $2h' = \widetilde{O}(\Delta_1^{1/2}\Delta_0^{1/2})$ by Lemmas 8.1 and 3.5. In particular, steps 4 and 5 take time $\widetilde{O}(\Delta_1^{1/2}\Delta_0^{1/2})$.

We now come to the most costly step. By Theorem 7.16, it takes time $\widetilde{O}(r_j^2)$ to do a single iteration of step 6a. In particular, all iterations of this step together take time $\widetilde{O}(\Delta_1^{7/2}\Delta_0^{11/2})$.

The $j$-th iteration of step 6b takes time $\widetilde{O}(r)$ and hence all iterations of this step together take time $\widetilde{O}(\Delta_1^2\Delta_0^3)$. Finally, by Theorem 10.5, step 7a takes time $\widetilde{O}(h')$ times $\widetilde{O}(p)$, which is $\widetilde{O}(\Delta_1^2\Delta_0^3)$. The same amount of time is needed for the final two steps.

The output consists of $h' + 1$ rational coefficients, each of which has a bit size of $\widetilde{O}(\Delta_1^{3/2}\Delta_0^{5/2})$, hence the size of the output is $\widetilde{O}(\Delta_1^2\Delta_0^3)$.

This proves the main theorem, except when using the polynomials $\widehat{H}_{K,n}$ $(n = 2, 3)$ of Section 2.2. With the naive method of evaluating $\widehat{H}_{K,n}$ that we described in Algorithm 11.1, it takes $\widetilde{O}(h_1)$ times as much time to evaluate $\widetilde{H}_{K,n}$ from the Igusa invariants as it does to evaluate $H_{K,n}$. This $\widetilde{O}(\Delta_1^{5/2}\Delta_0^{7/2})$ is still dominated by the running time of the rest of the algorithm. □

It also follows that, if one uses Dupont's [20] quasi-linear method of evaluating theta constants as mentioned in Section 7.4, the heuristic running time of Algorithm 11.1 is $\widetilde{O}(\Delta_1^2\Delta_0^3)$, which can still be improved if better bounds on the denominators are found. In fact, if we also use a guess for the height of the class polynomials, then we can compute class polynomials in *quasi-linear* time without proof of correctness.

If the goal is to construct a genus-two curve $C/k$ with a point $P \in J(C)(k)$ of prime order $N$ (as it is in the cryptographic applications), then correctness of the output $(C, P)$ can be proven efficiently afterwards by checking $P \neq [N]P = 0$. By doubling the precision every time the output is incorrect, and assuming Dupont's method is quasi-linear in the required precision, this yields a method that is quasi-linear in the bit size of the class polynomials.

# Chapter III

## The irreducible components of the CM locus

Abstract. *In this chapter, we show how to replace genus-2 class polynomials by smaller and more natural objects: the irreducible components of the CM-by-$K$ locus in the moduli space.*

In Chapter II, we gave an algorithm to compute the Igusa class polynomials of any primitive quartic CM-field $K$. Though Igusa class polynomials are the objects that are studied in the literature on explicit CM constructions of curves of genus 2, it is actually much better from a practical perspective to work with their irreducible factors over $K_0^{\mathrm{r}}$. We will explain why in Example 3.1 and Section 4 below.

At the same time, though Igusa class polynomials $H_{K,1}$, $\widehat{H}_{K,2}$, $\widehat{H}_{K,3}$ of $K$ in practice specify exactly what the abelian surfaces with CM by $\mathcal{O}_K$ are, and though in practice they define the field $CM_{K^{\mathrm{r}},\Phi^{\mathrm{r}}}$, this is not guaranteed, as the polynomial $H_{K,1}$ might not have a simple root. To get actual theorems about computing CM abelian surfaces or the field $\mathrm{CM}_{K^{\mathrm{r}},\Phi^{\mathrm{r}}}$, we will need to look at the moduli space of CM-by-$K$ points.

The current chapter combines these approaches: we study the irreducible components over $K_0^{\mathrm{r}}$ of the moduli space of CM-by-$K$ points. We then show what to change in the algorithms of Chapter II in order to compute these components.

We did not work directly with these irreducible components in Chap-

ter II to avoid making that chapter too heavy, and because Igusa class polynomials are the objects used in existing literature.

# 1 The moduli space of CM-by-$K$ points

The quotient $\mathrm{Sp}_{2g}(\mathbf{Z})\backslash\mathcal{H}_g$ of Section II.4 parametrizes the isomorphism classes of complex principally polarized abelian varieties of dimension $g$ in an analytic way. This *(coarse) moduli space* has an algebraic model $\mathcal{A}_g/\mathbf{Q}$ that parametrizes these isomorphism classes algebraically.

For $g = 1$, the variety $\mathcal{A}_g$ is simply the affine line $\mathbf{A}^1$ with the $j$-invariant as its coordinate. For $g = 2$, we take the moduli space $\mathcal{M}_2$ of curves of genus 2 and embed it into $\mathcal{A}_g$ by taking Jacobians. The space $\mathcal{M}_2$ is given in terms of the Igusa invariants of Section II.2 as the $I_{10} \neq 0$ locus of the 3-dimensional weighted projective space with coordinates $I_2, I_4, I_6, I_{10}$ (see Igusa [45]).

Let $K$ be a CM-field of degree $2g$ and $\Phi$ a CM-type of $K$ with values in $\overline{\mathbf{Q}} \subset \mathbf{C}$. We will restrict to primitive quartic CM-fields soon, but give general definitions now because we want to give an 8-dimensional example later. Let $(K^{\mathrm{r}}, \Phi^{\mathrm{r}})$ be the reflex of $(K, \Phi)$ and let $K_0^{\mathrm{r}}$ be the maximal totally real subfield of $K$. For the definitions, see Chapter I.

We define the CM-by-$(K, \Phi)$-locus $\mathcal{CM}_{K,\Phi} \subset \mathcal{A}_g(\overline{\mathbf{Q}})$ to be the set of points $A \in \mathcal{A}_g(\overline{\mathbf{Q}})$ such that there exists an embedding $\iota : \mathcal{O}_K \to \mathrm{End}(A)$ of type $\Phi$. Two CM-types $\Phi$ and $\Phi'$ of $K$ are called equivalent if there is an automorphism $\sigma$ of $K$ such that $\Phi' = \Phi\sigma$ holds. Recall from Section I.4 that $\mathcal{CM}_{K,\Phi}$ and $\mathcal{CM}_{K,\Phi'}$ coincide if $\Phi$ and $\Phi'$ are equivalent.

The CM-by-$K$-locus $\mathcal{CM}_K$ is the union of $\mathcal{CM}_{K,\Phi}$ over all equivalence classes of CM-types $\Phi$ of $K$.

**Lemma 1.1.** *The set $\mathcal{CM}_{K,\Phi}$ is finite and stable under* $\mathrm{Gal}(\overline{\mathbf{Q}}/K_0^{\mathrm{r}})$.

*Proof.* Finiteness is Proposition I.5.3. The set is stable under the action of $\mathrm{Gal}(\overline{\mathbf{Q}}/K^{\mathrm{r}})$ by the definition of $K^{\mathrm{r}}$ in Section I.4. It is stable under complex conjugation by Lemma I.9.2. □

# 2 The irreducible components of $\mathcal{CM}_{K,\Phi}$

Now let $K$ be a *primitive quartic* CM-field. As the CM-types of $K$ are primitive, we know that all abelian varieties with CM by $\mathcal{O}_K$ are simple (Theorem I.5.2.3), hence are Jacobians by Weil's Theorem I.6.3. In particular, the set $\mathcal{CM}_{K,\Phi}$ is contained in $\mathcal{M}_2 \subset \mathcal{A}_2$, hence can be given in terms of Igusa invariants.

**Lemma 2.1.** *If $K/\mathbf{Q}$ is cyclic quartic Galois, then all 4 CM-types $\Phi$ of $K$ are equivalent and we have $\mathcal{CM}_K = \mathcal{CM}_{K,\Phi}$.*

*If $K/\mathbf{Q}$ is quartic non-Galois, then there are two equivalence classes of CM-types $\Phi$ and $\Phi'$. The sets $\mathcal{CM}_{K,\Phi}$ and $\mathcal{CM}_{K,\Phi'}$ are disjoint, defined over the quadratic field $K_0^{\mathrm{r}}$ and Galois conjugate to each other.*

*Proof.* The equivalence classes of CM-types are given in Example I.7.5. The set $\mathcal{CM}_{K,\Phi}$ depends only on the equivalence class of $\Phi$ by 1.

In the non-Galois case, as $\Phi$ is primitive and not equivalent to $\Phi'$, we find that $\mathcal{CM}_{K,\Phi}$ and $\mathcal{CM}_{K,\Phi'}$ are disjoint by Lemma I.5.6. The fact that they are defined over $K_0^{\mathrm{r}}$ is Lemma 1.1.

Finally, if $\sigma \in \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ is non-trivial on $K_0^{\mathrm{r}}$, then $\sigma\circ\Phi$ is equivalent to $\Phi'$, hence by Lemma I.4.2, we have $\sigma\mathcal{CM}_{K,\Phi} = \mathcal{CM}_{K,\sigma\Phi} = \mathcal{CM}_{K,\Phi'}$. □

Let $G = \mathrm{Gal}(\overline{\mathbf{Q}}/K_0^{\mathrm{r}})$. We partition the set $\mathcal{CM}_{K,\Phi}$ into its $G$-orbits $B_1, \ldots, B_n$. Each $B_i$ can be defined in terms of equations with coefficients in $K_0^{\mathrm{r}}$. Note that these $G$-orbits are irreducible over $K^{\mathrm{r}}$ by Corollary I.9.3. These orbits do not have an analogue in the genus-one case, since the action of $\mathrm{Gal}(\overline{K}/K)$ on $\mathcal{CM}_K$ is transitive there.

In the case $n \geq 2$, a set of defining equations for $B_i$ can be smaller and easier to handle than a set of defining equations for all of $\mathcal{CM}_K$ or all of $\mathcal{CM}_{K,\Phi}$. Moreover, there are advantages of working with $B_i$ or $\mathcal{CM}_{K,\Phi}$ as opposed to $\mathcal{CM}_K$, as we will see in Section 4.

The following result was observed experimentally together with Andreas Enge while looking at the ECHIDNA database [50].

**Theorem 2.2.** *Let $K$ be a primitive* quartic *CM-field. Then the number of irreducible components of $\mathcal{CM}_{K,\Phi}$ over $K_0^{\mathrm{r}}$ is a power of* 2.

*Proof.* As we just mentioned, by Corollary I.9.3, the irreducible components over $K^{\mathrm{r}}$ are exactly the irreducible components over $K_0^{\mathrm{r}}$. The set $\mathcal{CM}_{K,\Phi}$ is non-empty because the union $\mathcal{CM}_K$ of $\mathcal{CM}_{K,\Phi}$ and its Galois conjugate $\mathcal{CM}_{K,\Phi'}$ is non-empty by Proposition I.5.3.

Let $S_+$ be the group of pairs $(\mathfrak{a}, u)$ with $\mathfrak{a}$ a fractional $\mathcal{O}_K$-ideal and $u \in K_0^*$ a totally positive element such that $\mathfrak{a}\overline{\mathfrak{a}} = u\mathcal{O}_K$. Then we have a natural homomorphism $K^* \to S_+$ given by $v \mapsto (v\mathcal{O}_K, v\overline{v})$. Let $C_+ = S_+/K^*$ be the set of $K^*$-orbits. The set of equivalence classes of triples $(\Phi, \mathfrak{a}, \xi)$ from Section I.5.2 with $\Phi$ fixed and $\mathfrak{a}, \xi$ varying is a $C_+$-torsor under the action

$$(\mathfrak{b}, u) \cdot (\Phi, \mathfrak{a}, \xi) = (\Phi, \mathfrak{b}^{-1}\mathfrak{a}, u\xi).$$

(see the proof of Proposition I.5.3.) In particular, it suffices to show that the cokernel of the (Galois) map

$$\begin{aligned} \mathrm{Cl}_{K^{\mathrm{r}}} &\to C_+ \\ \mathfrak{b} &\mapsto (N_{\Phi^{\mathrm{r}}}(\mathfrak{b}), N_{K^{\mathrm{r}}/\mathbf{Q}}(\mathfrak{b}))K^* \end{aligned} \tag{2.3}$$

from the main theorem of complex multiplication (I.9.1) has order a power of 2.

We claim that this cokernel has exponent 1 or 2. Let $(\mathfrak{a}, u)K^* \in C_+$ be any element. It suffices to show that $(\mathfrak{a}^2, u^2)K^*$ is in the image of the map (2.3).

Let $\mathfrak{b} = N_\Phi(\mathfrak{a})$. Then Lemma I.8.4 gives

$$\begin{aligned} (N_{\Phi^{\mathrm{r}}}(\mathfrak{b}), N_{K^{\mathrm{r}}/\mathbf{Q}}(\mathfrak{b})) &= (N_{K/\mathbf{Q}}(\mathfrak{a})\mathfrak{a}\overline{\mathfrak{a}}^{-1}, N_{K/\mathbf{Q}}(\mathfrak{a})^2) \\ &= N_{K/\mathbf{Q}}(\mathfrak{a})u^{-1}(\mathfrak{a}^2, u^2), \end{aligned}$$

which proves that $(\mathfrak{a}^2, u^2)K^*$ is in the image. □

# 3 Computing the irreducible components

Let $K$ be a primitive quartic CM-field. In Section II.2, we defined Igusa class polynomials by taking products and sums over all of $\mathcal{CM}_K$. To work with only one orbit $B_i$ for $G = \mathrm{Gal}(\overline{\mathbf{Q}}/K^{\mathrm{r}})$, there are two things that need to change in the algorithm of Chapter II:

1. we need to find all triples $(\Phi, \mathfrak{a}, \xi)$ corresponding to a single $G$-orbit, and

2. we need to be able to recognize coefficients in $K_0^{\mathrm{r}}$ instead of $\mathbf{Q}$.

For item 1, we can use the explicit Galois action in the main theorem of complex multiplication (I.9.1). So we can find exactly all triples $(\Phi, \mathfrak{a}, \xi)$ corresponding to a single $G$-orbit $B_i$ by computing

a. one such triple $(\Phi, \mathfrak{a}, \xi)$,

b. the class group $\mathrm{Cl}_{K^{\mathrm{r}}}$ of the reflex field, and

c. the reflex type norm map $N_{\Phi^{\mathrm{r}}} : \mathrm{Cl}_{K^{\mathrm{r}}} \to \mathrm{Cl}_K$.

For item 2, if we work with sufficiently high precision, we can use the LLL-algorithm to recover elements of $K_0^{\mathrm{r}}$ from their approximations $a$. Indeed, we can take a $\mathbf{Q}$-basis $\{1, \sqrt{D}\}$ of $K_0^{\mathrm{r}}$. Then we need to find integers $d, x, y$ such that $|x + y\sqrt{D} - ad|$ is small and $|x|, |y|, |d|$ are

not too large. This amounts to finding short vectors in a lattice, and can be done using the LLL-algorithm [55, 57]. As we know bounds on the denominators from Section II.9, we can make the required precision effective. This shows that we can adapt the algorithms of Chapter II to make the main theorem of that chapter valid also when restricting to a single $G$-orbit $B_i$. This solves item 2.

A potential other method for dealing with item 2 is the following. Write $K_0^{\mathrm{r}} = \mathbf{Q}(\sqrt{D})$ and let $\sigma$ be a generator of $\mathrm{Gal}(K_0^{\mathrm{r}}/\mathbf{Q})$. We know how to find the $\mathrm{Gal}(\overline{\mathbf{Q}}/K_0^{\mathrm{r}})$-orbits $B_1, \ldots, B_n$, but we do not know how to tell which of those orbits are $\sigma$-conjugate. There is a more general version of the explicit Galois action on CM abelian varieties that describes the action of *all* elements of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$, but we do not know how to make that explicit in terms of the triples $(\Phi, \mathfrak{a}, \xi)$ (see [52, Chapter 7] or [64, Thm. 10.1]).

Let $F$ be an Igusa class polynomial for $B_i$. Suppose we do know how to compute the set of triples $(\Phi, \mathfrak{a}, \xi)$ of $\sigma B_i$ from the set of triples of $B_i$. (Alternatively, we can simply guess $\sigma B_i = B_j$ for different $j$ and recognize good output since Igusa class polynomials have smooth denominators.) From $\sigma B_i$, compute $\sigma F$, and hence the *rational* polynomials $a = (F + \sigma F)/2$ and $b = (F - \sigma F)/(2\sqrt{D})$. We then have $F = a + b\sqrt{D}$.

**Example 3.1.** Consider the non-Galois quartic CM-field

$$K = \mathbf{Q}\left(\sqrt{-62 + 10\sqrt{5}}\right),$$

and let $\Phi$ be a CM-type of $K$ with values in a field $L'$. The reflex field of $\Phi$ is the field

$$K^{\mathrm{r}} = \mathbf{Q}\left(\sqrt{-31 + 2w}\right) \subset L'$$

with $w \in L'$ the square root of 209 that belongs to $\Phi$ as in Example I.7.7.

We computed one of the irreducible components of $\mathcal{CM}_{K,\Phi}$ over $K_0^{\mathrm{r}} = \mathbf{Q}(w)$ using Magma [7]. It is given in terms of Igusa invariants $(i_1, i_2, i_3)$ of Chapter II by $H_1(i_1) = 0$ and $H_1'(i_1) i_n = \widehat{H}_n(i_1)$ for $n = 2, 3$, where the class polynomials $H_1, \widehat{H}_2, \widehat{H}_3$ are given in Figure III.1.

We also give the polynomial $H_1$ for the full CM locus $\mathcal{CM}_K$ (Figure III.2) so that its size can be compared. We use \ to continue a number on the next line. By restricting to $\mathcal{CM}_{K,\Phi}$, the degree gets cut in half, but the bit size of the coefficients doubles, since they are in a field of degree 2. Then by restricting to one of the two irreducible components, we save a factor 2 in both the degree and the bit sizes of the coefficients. This explains why $H_1$ for all of $\mathcal{CM}_K$ takes about 4 times as much space as $H_1$ for one component.

$$
\begin{aligned}
&41^4151^2H_1 = \ 64430176561X^2+\\
&\quad + (20597907860952412478318642 7w\\
&\qquad - 29778049956995241329241284 31)X\\
&\quad + \tfrac{1}{2}(-59897980589118212913593046203606 13w\\
&\qquad + 86593506017412522675907964506455189),\\
&2^5 41^6 151^4 \widehat{H}_2 =\\
&\quad (-24548245580121701228650503189935324 73w\\
&\qquad + 35488986976522847855248253994749432769)X\\
&\quad + 28768580464678570992891511300020790788865449w\\
&\quad - 41590254313734399390804519312894705291 5790897,\\
&2^4 41^6 151^4 \widehat{H}_3 =\\
&\quad (-46704828432019435152440758726755388043516900604046875w\\
&\qquad + 67520387199915666730272734726222866393517108062542 1875)X\\
&\quad + 67907986738555049580963834409203071465118943464792631729 6875w\\
&\quad - 98173437575685797734623005429722003053153991595781831026 71875.
\end{aligned}
$$

Figure III.1: The Igusa class polynomials for one irreducible component of $\mathcal{CM}_{K,\Phi}$ for $K = \mathbf{Q}(\sqrt{-62+10\sqrt{5}})$ and $\Phi$ a CM-type of $K$ with reflex field $\mathbf{Q}(\sqrt{-31+2w})$, where $w^2 = 209$.

$$
\begin{aligned}
&+ 26936790672734596158486088 9X^8\\
&- 33128880546035571578256427748821805963065110X^7\\
&+ 76072521983579848280305702412117348534564225618142067810310 1X^6\\
&- 20183684192885387086967314946167301449078514413060730932659 4 \ \backslash\\
&\quad 00091100X^5\\
&+ 13321535368680385604061004774793949619989302533495102852294 8 \ \backslash\\
&\quad 971180071435884X^4\\
&- 82934744856795474043600841677095887822577580826630155555635 3 \ \backslash\\
&\quad 6247717943492256000X^3\\
&+ 46433730651626381266827133428344644244745343618027265314945 7 \ \backslash\\
&\quad 8699071343804782750000X^2\\
&+ 73246201411102743443822559336784691302658439484889380136648 1 \ \backslash\\
&\quad 6435158346235571250000 00X\\
&+ 22009354930798263763199865293756584095684721013674490215682 0 \ \backslash\\
&\quad 9002148569562001562500000 0
\end{aligned}
$$

Figure III.2: This is $13^4 29^2 41^4 79^2 151^2 167^2 H_1$ for the field $K = \mathbf{Q}(\sqrt{-62+10\sqrt{5}})$.

**Example 3.2.** Let $w = \sqrt{13}$, and consider the non-Galois quartic CM-field $F = \mathbf{Q}(\sqrt{-27+4w})$. We have seen in Example I.10.4 that the class field $\mathrm{CM}_{F,\Psi}$ for any CM-type $\Psi$ of $F$ equals the Hilbert class field $H_F$ of $F$.

The reflex field of such a CM-type $\Psi$ is $K = \mathbf{Q}(\sqrt{-54+2\sqrt{521}})$ by Example I.7.7. Let $\Phi$ be any CM-type of $K$ with reflex field $F$. Then $(K, \Phi)$ is the reflex of $(F, \Psi)$ for some CM-type $\Psi$ of $F$.

Figure III.3 gives the Igusa class polynomial $H_1 \in F_0[X]$ for such a CM-type $\Phi$. Any root of this polynomial generates $H_F$ over $F$. In a naive implementation of the algorithm we have just described with 200 digits precision, computing $H_1$ took time less than 3 seconds in Magma V2.16-1 [7] on a standard PC.

$$
\begin{aligned}
101^2 H_1 = {} & 10201X^7 \\
& + (155205162116358647755w + 559600170220938887110)X^6 \\
& + (152407687697460195175920750535594152550w \\
& \quad + 549513732768094956258970636118192859400)X^5 \\
& + \tfrac{1}{2}(220190958003052373027262384843453804831783451387 5w \\
& \quad + 79390978947354318441530190893209731530112108821 25)X^4 \\
& + (104717526292739318284916458748089136759471044939557062 5w \\
& \quad + 377564410488220083286572934642975206938020009784573687 5)X^3 \\
& + \tfrac{1}{2}(907392914800494855136752991106041311116404713247380 60 \ \backslash \\
& \quad 7234375w \\
& \quad + 327165168130591119268893142372375309476346120037916993 \ \backslash \\
& \quad 8284375)X^2 \\
& + (150141660496565198600458802229712441133906505259050699 8 \ \backslash \\
& \quad 7454062500w \\
& \quad + 541343455503671907856059844455869398930835318514053659 \ \backslash \\
& \quad 78411062500)X \\
& + \tfrac{1}{2}(320854170291151322128777010521751890513120770505490 53 \ \backslash \\
& \quad 7777676328984375w \\
& \quad + 115685616293120067038709321144324285012570966768326545 \ \backslash \\
& \quad 9917987279296875) \in \mathbf{Q}(w)[X]
\end{aligned}
$$

Figure III.3: The Igusa class polynomial $H_1$ of the field $K = \mathbf{Q}(\sqrt{-54+2\sqrt{521}})$, when restricting to one CM-type $\Phi$ of $K$ with reflex field $\mathbf{Q}(\sqrt{-27+4w})$, where $w^2 = 13$.

To compute $H_F$ using Kummer theory, one needs to take a 7-th root of an element in the degree-24 number field $F(\zeta_7)$. On the same machine, with the Magma function `HilbertClassField`, it takes about 2 minutes to compute the Hilbert class field of $F$. This is a lot longer than the 3 seconds we needed for computing $H_1$. The output is the field $H_F = F[X]/P$ with

$$\begin{aligned} P = {} & X^7 + (-49w - 133)X^5 \\ & + (8036w - 10955)X^4 \\ & + (247401w - 880005)X^3 \\ & + \tfrac{1}{2}(24737797w - 68979519)X^2 \\ & + \tfrac{1}{2}(533791741w - 1896276501)X \\ & + \tfrac{1}{2}(6759148445w - 11784293007) \in F_0[X]. \end{aligned}$$

# 4 The CM method

Now let $g$ be an arbitrary positive integer again. Suppose we want to construct a $g$-dimensional abelian variety over a finite field with a prescribed *irreducible* characteristic polynomial $f$ of the Frobenius endomorphism. The field $K = \mathbf{Q}[X]/(f)$ is a CM-field of degree $2g$ and the constant coefficient $f(0) = p^m$ is a prime power.

Take any point $A$ of $\mathcal{CM}_K$ and look at the reduction $\widetilde{A}$ of $A$ modulo a prime $\mathfrak{P}/p$ of a field of definition $k \supset K^{\mathrm{r}}$ of $A$. Let $\Phi$ be the CM-type of $A$, and let $\mathrm{Frob} \in \mathrm{End}(\widetilde{A})$ be the Frobenius endomorphism. Then we have the following result.

**Theorem 4.1** (Shimura-Taniyama formula [78, Thm. 1 in §1])**.** *The morphism* Frob *is an element of the ring* $\mathcal{O}_K \subset \mathrm{End}(\widetilde{A})$ *and generates the ideal* $N_{\Phi^{\mathrm{r}}}(N_{k/K^{\mathrm{r}}}(\mathfrak{P}))$ *of* $\mathcal{O}_K$*.* □

**Corollary 4.2.** The abelian variety $\widetilde{A}$ is isomorphic over $\overline{\mathbf{F}_p}$ to an abelian variety with characteristic polynomial $f$ if and only if a power of $\pi = (X \bmod f) \in K$ generates the ideal $N_{\Phi^{\mathrm{r}}}(N_{k/K^{\mathrm{r}}}(\mathfrak{P}))$ of $\mathcal{O}_K$.

*Proof.* See Honda and Tate [84]. □

The corollary shows that, when doing CM constructions as above, it is good to first find out for which CM-type $\Phi$ the element $\pi$ generates the reflex type norm of an ideal and then restrict to $A \in \mathcal{CM}_{K,\Phi}$.

**Example 4.3.** Suppose we want to construct an abelian surface $A$ over the finite field of $q = p^k$ elements with a given Frobenius endomorphism $\pi$ in a non-Galois CM-field $K$. Let $\Phi$ be a CM-type of $K$.

A common case is that $p$ splits completely in $K$. Indeed, this is one of the only two unramified decomposition types of $p$ in $K$ for which $A$ is ordinary (Goren [34]). Moreover, this is what will happen by construction in Chapter IV.

If $p$ splits completely in $K$, then it factors as $p\mathcal{O}_K = \mathfrak{p}_1\overline{\mathfrak{p}_1}\mathfrak{p}_2\overline{\mathfrak{p}_2}$. The 4 primes $\mathfrak{q}/p$ of $K^{\mathrm{r}}$ have the 4 distinct type norms given up to complex conjugation by $N_{\Phi^{\mathrm{r}}}(\mathfrak{q}) = \mathfrak{p}_1\mathfrak{p}_2$ and $N_{\Phi^{\mathrm{r}}}(\mathfrak{q}) = \mathfrak{p}_1\overline{\mathfrak{p}_2}$. We thus find $N_{\Phi^{\mathrm{r}}}(\mathfrak{q})^k = \pi\mathcal{O}_K$ for at most one $\mathfrak{q}$. To get an abelian surface $A$ with Frobenius endomorphism $\pi$ (up to complex conjugation), it is essential that we reduce modulo a prime above such a prime $\mathfrak{q}$. This amounts to taking $A$ to be a point of

$$\mathcal{CM}_{K,\Phi} \mod (\mathfrak{q} \cap K_0^{\mathrm{r}}).$$

By Theorem 4.1, we know Frob to be a generator of $N_{\Phi^{\mathrm{r}}}(\mathfrak{q})^k$. This fact and the fact $\mathrm{Frob} \cdot \overline{\mathrm{Frob}} = p^k$ determine Frob uniquely up to roots of unity in $\mathcal{O}_K^*$. As non-Galois quartic CM-fields do not have non-trivial roots of unity, we find that Frob is determined uniquely up to $\pm 1$, that is, up to quadratic twists of $A$.

In Example 3.1, reducing modulo a prime above $\mathfrak{q}$ amounts to replacing $w \in K_0^{\mathrm{r}}$ by $(w \bmod \mathfrak{q}) \in \mathbf{F}_p$, and then taking a solution $(i_1, i_2, i_3) \in \mathbf{F}_{p^k}^3$ to $H_1(i_1) = 0$ and $i_n = \widehat{H}_n(i_1)/H_1'(i_1)$ for $n = 2, 3$.

For the prime $p = 2^{128} + 463$, which splits completely in $K$, there is a unique element $\pi \in \mathcal{O}_K$ with $\pi\overline{\pi} = p$ and such that $N_{K/\mathbf{Q}}(\pi - 1)$, which is the order of the corresponding abelian variety, is a prime times a small integer. For that element $\pi$, we have that $N_{K/\mathbf{Q}}(\pi - 1)$ is 4 times the prime

$$N = 2^{254} - 5632861158402111064848197526240511442172628827329154462023.$$

We computed the appropriate prime $\mathfrak{q}$ in $K^{\mathrm{r}}$ and found

$$w \equiv 247135999804258747492727825167682242163 \pmod{\mathfrak{q}}.$$

We substitute this root modulo $p$ in the class polynomials of Example 3.1, and find a solution

$$\begin{aligned} i1 &= 18666460357470136455602049848978231995 5, \\ i2 &= 24801536539879749348632653448450367765 8, \\ i3 &= 92979908727002348130966293837941380436 \in \mathbf{F}_p. \end{aligned}$$

Mestre's algorithm [61] (available in Magma [7]) allows us to construct a curve $C : y^2 = f(x)$ from this solution. Either the Jacobian of $C$ or the

Jacobian of its quadratic twist $C'$ has order $4N$. The quadratic twist is given by $C' : y^2 = cf(x)$ for a non-square $c \in \mathbf{F}_p$. By taking random points on the Jacobians of $C$ and $C'$ and multiplying them by $4N$, we can check which of the two has the appropriate number of points. We find that the Jacobian of the curve

$$\begin{aligned} C : y^2 = x^6 &+ 194876360407882453864339562084283578641x^4 \\ &+ 725076348445526069019506070391391068 41x^3 \\ &+ 215701338546912274238542720250901753991x^2 \\ &+ 149128889692643278587362953981454162789x \\ &+ 277144679648822640993017616187904126204 \end{aligned}$$

over $\mathbf{F}_p$ has a point of order $N$. In particular, the Frobenius endomorphism of this Jacobian is $\pi$.

**Example 4.4.** Let $l$ be an odd prime number and consider the field $K = \mathbf{Q}(\zeta)$ for a primitive $l$-th root of unity $\zeta$. Then $K$ is a CM-field of degree $l-1$ and we let $g = (l-1)/2$. We know one point in $\mathcal{CM}_K$ explicitly as the Jacobian of a hyperelliptic curve: the Jacobian $J(C)$ of the curve $C : y^2 = x^l + 1$ of genus $g$ given in Example I.6.1. We know by that example that $J(C)$ has type $\Phi = \{\zeta \mapsto \zeta^l : l = 1, \ldots, g\}$.

Suppose we want to use this curve to construct an abelian variety over a finite field with a prescribed Frobenius endomorphism $\pi \in K$. By Corollary 4.2, this is possible only if we can write a power of $\pi\mathcal{O}_K$ as a type norm for the reflex type $\Phi^{\mathrm{r}}$ of the CM-type $\Phi$.

Composing $\iota$ on the right with an automorphism $\sigma$ of $K$ replaces $\Phi$ by $\Phi \circ \sigma$ and $\Phi^{\mathrm{r}}$ by $\Phi^{\mathrm{r}} \circ \sigma^{-1}$. This does not change the possible values of $N_{\Phi^{\mathrm{r}}}$. We thus find that there is one "correct" equivalence class of CM-type $\Phi$.

**Example 4.5.** In Chapter IV, we construct Weil numbers $\pi$ as type norms with respect to the reflex of a CM-type $\Phi_1$. When that chapter was published as [26], we were unaware of Corollary 4.2.

Example 5.4 of that chapter uses the the curve

$$y^2 = x^{17} + 1.$$

We used random CM-types $\Phi_1$ of $\mathbf{Q}(\zeta_{17})$ for constructing $\pi$, and then tried to use the curve $C$ of Example 4.4 to construct an abelian variety with Frobenius endomorphism $\pi$. We found that with some CM-types $\Phi_1$, we always failed, while with others, we always succeeded.

The CM-type $\Phi_1 = \{\zeta_{17} \mapsto \zeta_{17}^k : k = 1, 3, 5, 6, 8, 10, 13, 15\}$ was one of the 'successful' ones. It turns out that this CM-type $\Phi_1$ is equivalent

to the type $\Phi$ of Example 4.4 above. Indeed, with $\sigma(\zeta_{17}) = \zeta_{17}^5$, we have $\Phi_1 = \Phi \circ \sigma$.

By Corollary 4.2, we could have started out with $\Phi$ immediately instead of trying random CM-types $\Phi_1$ until successful.

# 5 Double roots

In this section, let $K$ be a primitive *quartic* CM-field. The Igusa class polynomials $\widehat{H}_{K,2}$, $\widehat{H}_{K,3}$ of Section II.2.2 are useful only if $H_{K,1}$ has a simple root. In practice, it never seems to happen that $H_{K,1}$ has a non-simple root. This is not surprising as the coefficients grow exponentially with the degree of these polynomials.

If we want a *proven* algorithm for computing $\mathcal{CM}_{K,\Phi}$ or an irreducible factor, then this argument isn't strong enough. In this section, we prove the following results.

**Theorem 5.1.** *Algorithm II.11.1 can be adapted so that it computes a set of defining polynomials for $\mathcal{CM}_{K,\Phi}$ in time $\widetilde{O}(\Delta_1^{7/2}\Delta_0^{11/2})$ for any primitive quartic CM-field $K$ and CM-type $\Phi$. The output is given as a set of polynomial equations for the irreducible factors over $K_0^{\mathrm{r}}$.*

**Theorem 5.2.** *Algorithm II.11.1 can be adapted so that it computes the field $\mathrm{CM}_{K^{\mathrm{r}},\Phi^{\mathrm{r}}}$ of Chapter I in time $\widetilde{O}(\Delta_1^{7/2}\Delta_0^{11/2})$ for any primitive quartic CM-field $K$ and CM-type $\Phi$ of $K$.*

The output in Theorem 5.2 is an ordered set of generators and a minimal polynomial of each generator in terms of the earlier ones.

If $i_1(C)$ is distinct for all $C \in \mathcal{CM}_K$, then the field extension $\mathrm{CM}_{K^{\mathrm{r}},\Phi^{\mathrm{r}}}/K_0^{\mathrm{r}}$ is simply given over $K_0^{\mathrm{r}}$ by the polynomial $H_{K,1}$ for one $\mathrm{Gal}(\overline{\mathbf{Q}}/K_0^{\mathrm{r}})$-orbit in $\mathcal{CM}_{K,\Phi}$. If moreover $i_3(C)$ is non-zero for all $C \in \mathcal{CM}_K$, then the points of a component $B_j$ of $\mathcal{CM}_{K,\Phi} \subset \mathcal{M}_2$ are those points with $H_{K,1}(i_1) = 0$, $\widehat{H}_{K,n}(i_1) = i_n H'_{K,1}(i_1)$ for $n = 2, 3$, where the sums and products in the definitions of the class polynomials are restricted to $B_j$. In practice, this is the whole story, though it is not a proof. The rest of this section proves the theorems without these assumptions.

As explained in Section 3, we can restrict to the irreducible components of $\mathcal{CM}_{K,\Phi}$. Note that all $i_3(C)$'s for one component are Galois conjugate, so that one is zero if and only if all are. It is therefore possible to check $i_3(C) \neq 0$ simply by checking $H_{K,3}(0) = 0$. In particular, we can use the absolute invariants $(i_1, i_2, i_3)$ of Section II.2 if $i_3(C) \neq 0$,

and otherwise choose

$$(i_1, i_2, i_3) = \begin{cases} (I_2^2 I_6' I_{10}^{-1},\ I_6'^5 I_{10}^{-3},\ 0) & \text{if } I_4 = 0 \text{ and } I_6' \neq 0; \\ (I_2^5 I_{10}^{-1},\ 0,\ 0) & \text{if } I_4 = I_6' = 0. \end{cases} \tag{5.3}$$

This choice guarantees that every triple $(i_1, i_2, i_3)$ defines a *unique* point in $\mathcal{M}_2$. For details, see Cardona and Quer [12], who use similar invariants.

The polynomial $\widehat{H}_{K,2}$ gives a "modified Lagrange interpolation" for $i_2(C)$ in terms of $i_1(C)$. If more curves $C$ have the same $i_1$-value, then we can take the minimal polynomial $H_2^*$ of $i_2(C)$ over $\mathbf{Q}(i_1(C))$ and replace $\widehat{H}_{K,2}$ by a "modified Lagrange interpolation" of the *coefficients* of $H_2^*$ and do something similar for $i_3(C)$. The rest of the current section does that in a formal way.

Fix one element $C \in \mathcal{CM}_{K,\Phi}$, given by its triple $(\Phi, \mathfrak{a}, \xi)$. Let

$$G_0 = \mathrm{Gal}(\mathrm{CM}_{K^{\mathrm{r}},\Phi^{\mathrm{r}}}/K^{\mathrm{r}}) = I_{K^{\mathrm{r}}}/H_{K^{\mathrm{r}},\Phi^{\mathrm{r}}}$$

as in Section I.9. For any $g \in G_0$, we can compute $g(C)$ via the Galois action of the main theorem of complex multiplication I.9.1. We can then test $g(i_1(C)) = i_1(C)$ using the absolute value bounds on the conjugates on $i_1(C)$ and the denominator bound on the norm. In particular, we can compute the groups

$$\begin{aligned} G_1 &= \{g \in G_0 : g(i_1(C)) = i_1(C)\} \quad \text{and} \\ G_2 &= \{g \in G_1 : g(i_2(C)) = i_2(C)\}. \end{aligned}$$

Next, we define

$$\begin{aligned} H_1 &= \prod_{g \in G_0/G_1} (X - g(i_1(C))) && \in \mathbf{Q}[X] \subset \mathbf{C}[X], \\ H_2^* &= \prod_{g \in G_1/G_2} (X - g(i_2(C))) && \in \mathbf{Q}(i_1(C))[X] \subset \mathbf{C}[X], \\ H_3^{**} &= \prod_{g \in G_2} (X - g(i_3(C))) && \in \mathbf{Q}(i_1(C), i_2(C))[X] \subset \mathbf{C}[X]. \end{aligned}$$

We compute $H_1$ and approximate $gH_2^*$ for all $g \in G_0/G_1$ and $gH_3^{**}$ for all $g \in G_0/G_2$. Then let

$$\begin{aligned} H_2 &= \sum_{g \in G/G_1} (gH_2^*)(X_2) \prod_{\substack{h \in G_0/G_1 \\ h \neq g}} (X_1 - h(i_1(C))) && \in \mathbf{Q}[X_1, X_2], \\ H_3^* &= \sum_{g \in G_1/G_2} (gH_3^{**})(X_3) \prod_{\substack{h \in G_1/G_2 \\ h \neq g}} (X_2 - h(i_2(C))) && \in \mathbf{Q}(i_1(C))[X_2, X_3]. \end{aligned}$$

Again, we compute $H_2$ and approximate $gH_3^*$ for all $g \in G/G_1$.

Finally, let

$$H_3 = \sum_{g \in G/G_1} (gH_3^*)(X_2, X_3) \prod_{\substack{h \in G_0/G_1 \\ h \neq g}} (X_1 - h(i_1(C))) \in \mathbf{Q}[X_1, X_2, X_3].$$

Finally, we compute $H_3$. As all computations mentioned above can be done in the time mentioned in Theorem 5.1, the following lemma proves that theorem. □

**Lemma 5.4.** *The zero set of* $(H_1, H_2, H_3) \subset \mathbf{Q}[X_1, X_2, X_3]$ *in* $\overline{\mathbf{Q}}^3$ *is exactly the orbit of* $C \in \mathcal{CM}_{K,\Phi}$ *under the action of* $G = \mathrm{Gal}(\overline{\mathbf{Q}}/K^{\mathrm{r}})$.

*Proof.* The polynomial $H_1$ is the minimal polynomial of $C$, hence has as its roots exactly the values of $i_1(g(C))$ when $g$ ranges over $G$.

If we substitute one of these values $i_1^0 = i_1(g(C))$ for $X_1$, then $H_2$ becomes a univariate polynomial in $X = X_2$. In fact, this univariate polynomial is a non-zero constant times $gH_2^*$, hence its roots are the values of $ghi_2(C)$ where $h$ ranges over $G_1/G_2$. As $hG_1$ leaves $gi_1(C)$ invariant, the roots of $gH_2^*$ are exactly the values of $i_2$ corresponding to $i_1^0$.

Suppose we substitute one of these pairs $(i_1^0, i_2^0) = gh(i_1, i_2)(C)$ for $(X_1, X_2)$ in $H_3$. Then $H_3$ becomes a univariate polynomial in $X = X_3$. In fact, it becomes a non-zero constant times $H_3^{**}$. By the same argument as above, we find that the roots of this polynomial are exactly the $i_3$-values corresponding to our pair $(i_1^0, i_2^0)$.

As mentioned just below equation (5.3), the triples $(i_1, i_2, i_3)(g(C))$ determine $g(C)$ completely. □

*Proof of Theorem 5.2.* By Lemma 5.4, we have a tower of fields

$$K^{\mathrm{r}} \subset K^{\mathrm{r}}(i_1(C)) \subset K^{\mathrm{r}}(i_1(C), i_2(C)) \subset K^{\mathrm{r}}(i_1(C), i_2(C), i_3(C)),$$

where the minimal polynomials of $i_1(C)$, $i_2(C)$, and $i_3(C)$ are given by $H_1$, $H_2(i_1(C), X)$, and $H_3(i_1(C), i_2(C), X)$. As the largest field in this tower equals $\mathcal{CM}_{K^{\mathrm{r}},\Phi^{\mathrm{r}}}$, this proves Theorem 5.2. □

# Chapter IV

# Abelian varieties with prescribed embedding degree

This chapter appeared as David Freeman, Peter Stevenhagen, and Marco Streng, *Abelian Varieties with Prescribed Embedding Degree* [26] in *Algorithmic Number Theory*, ANTS-VIII, volume 5011 of Lecture Notes in Computer Science, 2008.

Abstract. *We present an algorithm that, on input of a CM-field $K$, an integer $k \geq 1$, and a prime $r \equiv 1 \bmod k$, constructs a $q$-Weil number $\pi \in \mathcal{O}_K$ corresponding to an ordinary, simple abelian variety $A$ over the field $\mathbf{F}$ of $q$ elements that has an $\mathbf{F}$-rational point of order $r$ and embedding degree $k$ with respect to $r$. We then discuss how CM-methods can be used to explicitly construct $A$.*

## 1 Introduction

Let $A$ be an abelian variety defined over a finite field $\mathbf{F}$, and $r \neq \mathrm{char}(\mathbf{F})$ a prime number dividing the order of the group $A(\mathbf{F})$. Then the *embedding degree* of $A$ with respect to $r$ is the degree of the field extension $\mathbf{F} \subset \mathbf{F}(\zeta_r)$ obtained by adjoining a primitive $r$-th root of unity $\zeta_r$ to $\mathbf{F}$.

The embedding degree is a natural notion in pairing-based cryptography, where $A$ is taken to be the Jacobian of a curve defined over $\mathbf{F}$.

In this case, $A$ is principally polarized and we have the non-degenerate *Weil pairing*

$$e_r : A[r] \times A[r] \longrightarrow \mu_r$$

on the subgroup scheme $A[r]$ of $r$-torsion points of $A$ with values in the $r$-th roots of unity. If $\mathbf{F}$ contains $\zeta_r$, we also have the non-trivial *Tate pairing*

$$t_r : A[r](\mathbf{F}) \times A(\mathbf{F})/rA(\mathbf{F}) \to \mathbf{F}^*/(\mathbf{F}^*)^r.$$

The Weil and Tate pairings can be used to 'embed' $r$-torsion subgroups of $A(\mathbf{F})$ into the multiplicative group $\mathbf{F}(\zeta_r)^*$, and thus the discrete logarithm problem in $A(\mathbf{F})[r]$ can be 'reduced' to the same problem in $\mathbf{F}(\zeta_r)^*$ [60, 29]. In pairing-based cryptographic protocols [67], one chooses the prime $r$ and the embedding degree $k$ such that the discrete logarithm problems in $A(\mathbf{F})[r]$ and $\mathbf{F}(\zeta_r)^*$ are computationally infeasible, and of roughly equal difficulty. This means that $r$ is typically large, whereas $k$ is small. Jacobians of curves meeting such requirements are often said to be *pairing-friendly*.

If $\mathbf{F}$ has order $q$, the embedding degree $k = [\mathbf{F}(\zeta_r) : \mathbf{F}]$ is simply the multiplicative order of $q$ in $(\mathbf{Z}/r\mathbf{Z})^*$. As 'most' elements in $(\mathbf{Z}/r\mathbf{Z})^*$ have large order, the embedding degree of $A$ with respect to a large prime divisor $r$ of $\#A(\mathbf{F})$ will usually be of the same size as $r$, and $A$ will not be pairing-friendly. One is therefore led to the question of how to efficiently construct $A$ and $\mathbf{F}$ such that $A(\mathbf{F})$ has a (large) prime factor $r$ and the embedding degree of $A$ with respect to $r$ has a prescribed (small) value $k$. The current paper addresses this question on two levels: the *existence* and the actual *construction* of $A$ and $\mathbf{F}$.

Section 2 focuses on the question whether, for given $r$ and $k$, there exist abelian varieties $A$ that are defined over a finite field $\mathbf{F}$, have an $\mathbf{F}$-rational point of order $r$, and have embedding degree $k$ with respect to $r$. We consider only abelian varieties $A$ that are *simple*, that is, not isogenous (over $\mathbf{F}$) to a product of lower-dimensional varieties, as we can always reduce to this case. By Honda-Tate theory [84], isogeny classes of simple abelian varieties $A$ over the field $\mathbf{F}$ of $q$ elements are in one-to-one correspondence with $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$-conjugacy classes of $q$-*Weil numbers*, which are algebraic integers $\pi$ with the property that all embeddings of $\pi$ into $\mathbf{C}$ have absolute value $\sqrt{q}$. This correspondence is given by the map sending $A$ to its $q$-th power Frobenius endomorphism $\pi$ inside the number field $\mathbf{Q}(\pi) \subset \mathrm{End}(A) \otimes \mathbf{Q}$. The existence of abelian varieties with the properties we want is thus tantamount to the existence of suitable Weil numbers.

Our main result, Algorithm 2.12, constructs suitable $q$-Weil numbers $\pi$ in a given *CM-field* $K$. It exhibits $\pi$ as a *type norm* of an element in

a *reflex field* of $K$ satisfying certain congruences modulo $r$. The abelian varieties $A$ in the isogeny classes over $\mathbf{F}$ that correspond to these Weil numbers have an $\mathbf{F}$-rational point of order $r$ and embedding degree $k$ with respect to $r$. Moreover, they are *ordinary*, i.e., $\#A(\overline{\mathbf{F}})[p] = p^g$, where $p$ is the characteristic of $\mathbf{F}$. Theorem 3.1 shows that for fixed $K$, the expected run time of our algorithm is heuristically polynomial in $\log r$.

For an abelian variety of dimension $g$ over the field $\mathbf{F}$ of $q$ elements, the group $A(\mathbf{F})$ has roughly $q^g$ elements, and one compares this size to $r$ by setting

$$\rho = \frac{g \log q}{\log r}. \tag{1.1}$$

In cryptographic terms, $\rho$ measures the ratio of a pairing-based system's required bandwidth to its security level, so small $\rho$-values are desirable. *Supersingular* abelian varieties can achieve $\rho$-values close to 1, but their embedding degrees are limited to a few values that are too small to be practical [30, 69]. Theorem 3.4 discusses the distribution of the (larger) $\rho$-values we obtain.

In Section 4, we address the issue of the actual construction of abelian varieties corresponding to the Weil numbers found by our algorithm. This is accomplished via the construction in characteristic zero of the abelian varieties having CM by the ring of integers $\mathcal{O}_K$ of $K$, a hard problem that is far from being algorithmically solved. We discuss the elliptic case $g = 1$, for which reasonable algorithms exist, and the case $g = 2$, for which such algorithms are still in their infancy. For genus $g \geq 3$, we restrict attention to a few families of curves that we can handle at this point. Our final Section 5 provides numerical examples.

# 2 Weil numbers yielding prescribed embedding degrees

Let $\mathbf{F}$ be a field of $q$ elements, $A$ a $g$-dimensional simple abelian variety over $\mathbf{F}$, and $K = \mathbf{Q}(\pi) \subset \mathrm{End}(A) \otimes \mathbf{Q}$ the number field generated by the Frobenius endomorphism $\pi$. Then $\pi$ is a *$q$-Weil number* in $K$: an algebraic integer with the property that all of its embeddings in $\overline{\mathbf{Q}}$ have complex absolute value $\sqrt{q}$.

The $q$-Weil number $\pi$ determines the group order of $A(\mathbf{F})$: the $\mathbf{F}$-rational points of $A$ form the kernel of the endomorphism $\pi - 1$, and in the case where $K = \mathbf{Q}(\pi)$ is the full endomorphism algebra $\mathrm{End}(A) \otimes \mathbf{Q}$ we have

$$\#A(\mathbf{F}) = \mathrm{N}_{K/\mathbf{Q}}(\pi - 1).$$

In the case $K = \mathrm{End}(A) \otimes \mathbf{Q}$ we will focus on, $K$ is a *CM-field* of degree $2g$ as in [84, Section 1], i.e., a totally complex quadratic extension of a totally real subfield $K_0 \subset K$.

**Proposition 2.1.** *Let $A$, $\mathbf{F}$ and $\pi$ be as above, and assume $K = \mathbf{Q}(\pi)$ equals $\mathrm{End}_{\mathbf{F}}(A) \otimes \mathbf{Q}$. Let $k$ be a positive integer, $\Phi_k$ the $k$-th cyclotomic polynomial, and $r \nmid qk$ a prime number. If we have*

$$\begin{aligned} \mathrm{N}_{K/\mathbf{Q}}(\pi - 1) &\equiv 0 \pmod{r}, \\ \Phi_k(\pi\overline{\pi}) &\equiv 0 \pmod{r}, \end{aligned}$$

*then $A$ has embedding degree $k$ with respect to $r$.*

*Proof.* The first condition tells us that $r$ divides $\#A(\mathbf{F})$, the second that the order of $\pi\overline{\pi} = q$ in $(\mathbf{Z}/r\mathbf{Z})^*$, which is the embedding degree of $A$ with respect to $r$, equals $k$. □

By Honda-Tate theory [84], all $q$-Weil numbers arise as Frobenius elements of abelian varieties over $\mathbf{F}$. Thus, we can prove the *existence* of an abelian variety $A$ as in Proposition 2.1 by exhibiting a $q$-Weil number $\pi \in K$ as in that proposition. The following lemma states what we need.

**Lemma 2.2.** *Let $\pi$ be a $q$-Weil number. Then there exists a unique isogeny class of simple abelian varieties $A/\mathbf{F}$ with Frobenius $\pi$. If $K = \mathbf{Q}(\pi)$ is totally imaginary of degree $2g$ and $q$ is prime, then such $A$ have dimension $g$, and $K$ is the full endomorphism algebra $\mathrm{End}_{\mathbf{F}}(A) \otimes \mathbf{Q}$. If furthermore $q$ is unramified in $K$, then $A$ is ordinary.*

*Proof.* The main theorem of [84] yields existence and uniqueness, and shows that $E = \mathrm{End}_{\mathbf{F}}(A) \otimes \mathbf{Q}$ is a central simple algebra over $K = \mathbf{Q}(\pi)$ satisfying

$$2 \cdot \dim(A) = [E : K]^{\frac{1}{2}} [K : \mathbf{Q}].$$

For $K$ totally imaginary of degree $2g$ and $q$ prime, Waterhouse [92, Theorem 6.1] shows that we have $E = K$ and $\dim(A) = g$. By [92, Prop. 7.1], $A$ is ordinary if and only if $\pi + \overline{\pi}$ is prime to $q = \pi\overline{\pi}$ in $\mathcal{O}_K$. Thus if $A$ is not ordinary, the ideals $(\pi)$ and $(\overline{\pi})$ have a common divisor $\mathfrak{p} \subset \mathcal{O}_K$ with $\mathfrak{p}^2 \mid q$, so $q$ ramifies in $K$. □

**Example 2.3.** Our general construction is motivated by the case where $K$ is a Galois CM-field of degree $2g$, with cyclic Galois group generated by $\sigma$. Here $\sigma^g$ is complex conjugation, so we can construct an element $\pi \in \mathcal{O}_K$ satisfying $\pi\sigma^g(\pi) = \pi\overline{\pi} \in \mathbf{Z}$ by choosing any $\xi \in \mathcal{O}_K$ and

letting $\pi = \prod_{i=1}^{g} \sigma^i(\xi)$. For such $\pi$, we have $\pi\overline{\pi} = N_{K/\mathbf{Q}}(\xi) \in \mathbf{Z}$. If $N_{K/\mathbf{Q}}(\xi)$ is a prime $q$, then $\pi$ is a $q$-Weil number in $K$.

Now we wish to impose the conditions of Proposition 2.1 on $\pi$. Let $r$ be a rational prime that splits completely in $K$, and $\mathfrak{r}$ a prime of $\mathcal{O}_K$ over $r$. For $i = 1, \ldots, 2g$, put $\mathfrak{r}_i = \sigma^{-i}(\mathfrak{r})$; then the factorization of $r$ in $\mathcal{O}_K$ is $r\mathcal{O}_K = \prod_{i=1}^{2g} \mathfrak{r}_i$. If $\alpha_i \in \mathbf{F}_r = \mathcal{O}_K/\mathfrak{r}_i$ is the residue class of $\xi$ modulo $\mathfrak{r}_i$, then $\sigma^i(\xi)$ modulo $\mathfrak{r}$ is also $\alpha_i$, so the residue class of $\pi$ modulo $\mathfrak{r}$ is $\prod_{i=1}^{g} \alpha_i$. Furthermore, the residue class of $\pi\overline{\pi}$ modulo $\mathfrak{r}$ is $\prod_{i=1}^{2g} \alpha_i$. If we choose $\xi$ to satisfy

$$\prod_{i=1}^{g} \alpha_i = 1 \in \mathbf{F}_r, \tag{2.4}$$

we find $\pi \equiv 1 \pmod{\mathfrak{r}}$ and thus $N_{K/\mathbf{Q}}(\pi - 1) \equiv 0 \pmod{r}$. By choosing $\xi$ such that in addition

$$\zeta = \prod_{i=1}^{2g} \alpha_i = \prod_{i=g+1}^{2g} \alpha_i \tag{2.5}$$

is a primitive $k$-th root of unity in $\mathbf{F}_r^*$, we guarantee that $\pi\overline{\pi} = q$ is a primitive $k$-th root of unity modulo $r$. Thus we can try to find a Weil number as in Proposition 2.1 by picking residue classes $\alpha_i \in \mathbf{F}_r^*$ for $i = 1, \ldots, 2g$ meeting the two conditions above, computing some 'small' lift $\xi \in \mathcal{O}_K$ with $(\xi \bmod \mathfrak{r}_i) = \alpha_i$, and testing whether $\pi = \prod_{i=1}^{g} \sigma^i(\xi)$ has prime norm. As numbers of moderate size have a high probability of being prime by the prime number theorem, a small number of choices $(\alpha_i)_i$ should suffice. There are $(r-1)^{2g-2}\varphi(k)$ possible choices for $(\alpha_i)_{i=1}^{2g}$, where $\varphi$ is the Euler totient function, so for $g > 1$ and large $r$ we are very likely to succeed. For $g = 1$, there are only a few choices $(\alpha_1, \alpha_2) = (1, \zeta)$, but one can try various lifts and thus recover what is known as the Cocks-Pinch algorithm [25, Theorem 4.1] for finding pairing-friendly elliptic curves. □

For arbitrary CM-fields $K$, the appropriate generalization of the map

$$\xi \mapsto \prod_{i=1}^{g} \sigma^i(\xi)$$

in Example 2.3 is provided by the *type norm*. A *CM-type* of a CM-field $K$ of degree $2g$ is a set $\Phi = \{\phi_1, \ldots, \phi_g\}$ of embeddings of $K$ into its normal closure $L$ such that $\Phi \cup \overline{\Phi} = \{\phi_1, \ldots, \phi_g, \overline{\phi_1}, \ldots, \overline{\phi_g}\}$ is the complete set of embeddings of $K$ into $L$. The *type norm* $N_\Phi : K \to L$ with respect to $\Phi$ is the map

$$N_\Phi : x \longmapsto \prod_{i=1}^{g} \phi_i(x),$$

which clearly satisfies

$$N_\Phi(x)\overline{N_\Phi(x)} = N_{K/\mathbf{Q}}(x) \in \mathbf{Q}. \tag{2.6}$$

If $K$ is not Galois, the type norm $N_\Phi$ does not map $K$ to itself, but to its *reflex field* $\widehat{K}$ with respect to $\Phi$. To end up in $K$, we can however take the type norm with respect to the *reflex type* $\Psi$, which we will define now (cf. [77, Section 8]).

Let $G$ be the Galois group of $L/\mathbf{Q}$, and $H$ the subgroup fixing $K$. Then the $2g$ left cosets of $H$ in $G$ can be viewed as the embeddings of $K$ in $L$, and this makes the CM-type $\Phi$ into a set of $g$ left cosets of $H$ for which we have $G/H = \Phi \cup \overline{\Phi}$. Let $S$ be the union of the left cosets in $\Phi$, and put $\widehat{S} = \{\sigma^{-1} : \sigma \in S\}$. Let $\widehat{H} = \{\gamma \in G : \gamma S = S\}$ be the stabilizer of $S$ in $G$. Then $\widehat{H}$ defines a subfield $\widehat{K}$ of $L$, and as we have $\widehat{H} = \{\gamma \in G : \widehat{S}\gamma = \widehat{S}\}$ we can interpret $\widehat{S}$ as a union of left cosets of $\widehat{H}$ inside $G$. These cosets define a set of embeddings $\Psi$ of $\widehat{K}$ into $L$. We call $\widehat{K}$ the *reflex field* of $(K, \Phi)$ and we call $\Psi$ the *reflex type*.

**Lemma 2.7.** *The field $\widehat{K}$ is a CM-field. It is generated over $\mathbf{Q}$ by the sums $\sum_{\phi\in\Phi} \phi(x)$ for $x \in K$, and $\Psi$ is a CM-type of $\widehat{K}$. The type norm $N_\Phi$ maps $K$ to $\widehat{K}$.*

*Proof.* The first two statements are proved in [77, Chapter II, Proposition 28] (though the definition of $\widehat{H}$ differs from ours, because Shimura lets $G$ act from the right). For the last statement, notice that for $\gamma \in \widehat{H}$, we have $\gamma S = S$, so $\gamma \prod_{\phi\in\Phi} \phi(x) = \prod_{\phi\in\Phi} \phi(x)$. □

A CM-type $\Phi$ of $K$ is *induced* from a CM-subfield $K' \subset K$ if it is of the form $\Phi = \{\phi : \phi|_{K'} \in \Phi'\}$ for some CM-type $\Phi'$ of $K'$. In other words, $\Phi$ is induced from $K'$ if and only if $S$ as above is a union of left cosets of $\mathrm{Gal}(L/K')$. We call $\Phi$ *primitive* if it is not induced from a strict subfield of $K$; primitive CM-types correspond to simple abelian varieties [77]. Notice that the reflex type $\Psi$ is primitive by definition of $\widehat{K}$, and that $(K, \Phi)$ is induced from the reflex of its reflex. In particular, if $\Phi$ is primitive, then the reflex of its reflex is $(K, \Phi)$ itself. For $K$ Galois and $\Phi$ primitive we have $\widehat{K} = K$, and the reflex type of $\Phi$ is $\Psi = \{\phi^{-1} : \phi \in \Phi\}$.

For CM-fields $K$ of degree 2 or 4 with primitive CM-types, the reflex field $\widehat{K}$ has the same degree as $K$. This fails to be so for $g \geq 3$.

**Lemma 2.8.** *If $K$ has degree $2g$, then the degree of $\widehat{K}$ divides $2^g g!$.*

*Proof.* We have $K = K_0(\sqrt{\eta})$, with $K_0$ totally real and $\eta \in K$ totally negative. The normal closure $L$ of $K$ is obtained by adjoining to the normal closure $\widetilde{K_0}$ of $K_0$, which has degree dividing $g!$, the square roots of the $g$ conjugates of $\eta$. Thus $L$ is of degree dividing $2^g g!$, and $\widehat{K}$ is a subfield of $L$. □

For a 'generic' CM-field $K$ the degree of $L$ is exactly $2^g g!$, and $\widehat{K}$ is a field of degree $2^g$ generated by $\sum_\sigma \sqrt{\sigma(\eta)}$, with $\sigma$ ranging over $\mathrm{Gal}(K_0/\mathbf{Q})$.

From (2.6) and Lemma 2.7, we find that for every $\xi \in \mathcal{O}_{\widehat{K}}$, the element $\pi = N_\Psi(\xi)$ is an element of $\mathcal{O}_K$ that satisfies $\pi\overline{\pi} \in \mathbf{Z}$. To make $\pi$ satisfy the conditions of Proposition 2.1, we need to impose conditions modulo $r$ on $\xi$ in $\widehat{K}$. Suppose $r$ splits completely in $K$, and therefore in its normal closure $L$ and in the reflex field $\widehat{K}$ with respect to $\Phi$. Pick a prime $\mathfrak{R}$ over $r$ in $L$, and write $\mathfrak{r}_\psi = \psi^{-1}(\mathfrak{R}) \cap \mathcal{O}_{\widehat{K}}$ for $\psi \in \Psi$. Then the factorization of $r$ in $\mathcal{O}_{\widehat{K}}$ is

$$r\mathcal{O}_{\widehat{K}} = \prod_{\psi\in\Psi} \mathfrak{r}_\psi \overline{\mathfrak{r}_\psi}. \tag{2.9}$$

**Theorem 2.10.** *Let $(K, \Phi)$ be a CM-type and $(\widehat{K}, \Psi)$ its reflex. Let $r \equiv 1 \pmod{k}$ be a prime that splits completely in $K$, and write its factorization in $\mathcal{O}_{\widehat{K}}$ as in (2.9). Given $\xi \in \mathcal{O}_{\widehat{K}}$, write $(\xi \bmod \mathfrak{r}_\psi) = \alpha_\psi \in \mathbf{F}_r$ and $(\xi \bmod \overline{\mathfrak{r}_\psi}) = \beta_\psi \in \mathbf{F}_r$ for $\psi \in \Psi$. If we have*

$$\prod_{\psi\in\Psi} \alpha_\psi = 1 \qquad \text{and} \qquad \prod_{\psi\in\Psi} \beta_\psi = \zeta \tag{2.11}$$

*for some primitive $k$-th root of unity $\zeta \in \mathbf{F}_r^*$, then $\pi = N_\Psi(\xi) \in \mathcal{O}_K$ satisfies $\pi\overline{\pi} \in \mathbf{Z}$ and*

$$\begin{aligned} \mathrm{N}_{K/\mathbf{Q}}(\pi - 1) &\equiv 0 \pmod{r}, \\ \Phi_k(\pi\overline{\pi}) &\equiv 0 \pmod{r}. \end{aligned}$$

*Proof.* This is a straightforward generalization of the argument in Example 2.3. The conditions (2.11) generalize (2.4) and (2.5), and imply in the present context that $\pi - 1 \in \mathcal{O}_K$ and $\Phi_k(\pi\overline{\pi}) \in \mathbf{Z}$ are in the prime $\mathfrak{R} \subset \mathcal{O}_L$ over $r$ that underlies the factorization (2.9). □

If the element $\pi$ in Theorem 2.10 generates $K$ and $\mathrm{N}_{K/\mathbf{Q}}(\pi)$ is a prime $q$ that is unramified in $K$, then by Lemma 2.2 $\pi$ is a $q$-Weil number corresponding to an ordinary abelian variety $A$ over $\mathbf{F} = \mathbf{F}_q$ with endomorphism algebra $K$ and Frobenius element $\pi$. By Proposition 2.1, $A$ has embedding degree $k$ with respect to $r$. This leads to the following algorithm.

---

**Algorithm 2.12.**
**Input:** a CM-field $K$ of degree $2g \geq 4$, a primitive CM-type $\Phi$ of $K$, a positive integer $k$, and a prime $r \equiv 1 \pmod{k}$ that splits completely in $K$.
**Output:** a prime $q$ and a $q$-Weil number $\pi \in K$ corresponding to an

ordinary, simple abelian variety $A/\mathbf{F}$ with embedding degree $k$ with respect to $r$.

---

1. Compute a Galois closure $L$ of $K$ and the reflex $(\widehat{K}, \Psi)$ of $(K, \Phi)$. Set $\widehat{g} \leftarrow \frac{1}{2} \deg \widehat{K}$ and write $\Psi = \{\psi_1, \psi_2, \ldots, \psi_{\widehat{g}}\}$.
2. Fix a prime $\mathfrak{R} \mid r$ of $\mathcal{O}_L$, and compute the factorization of $r$ in $\mathcal{O}_{\widehat{K}}$ as in (2.9).
3. Compute a primitive $k$-th root of unity $\zeta \in \mathbf{F}_r^*$.
4. Choose random $\alpha_1, \ldots, \alpha_{\widehat{g}-1}, \beta_1, \ldots, \beta_{\widehat{g}-1} \in \mathbf{F}_r^*$.
5. Set $\alpha_{\widehat{g}} \leftarrow \prod_{i=1}^{\widehat{g}-1} \alpha_i^{-1} \in \mathbf{F}_r^*$ and $\beta_{\widehat{g}} \leftarrow \zeta \prod_{i=1}^{\widehat{g}-1} \beta_i^{-1} \in \mathbf{F}_r^*$.
6. Compute $\xi \in \mathcal{O}_{\widehat{K}}$ such that $(\xi \mod \mathfrak{r}_{\psi_i}) = \alpha_i$ and $(\xi \mod \overline{\mathfrak{r}_{\psi_i}}) = \beta_i$ for $i = 1, 2, \ldots, \widehat{g}$.
7. Set $q \leftarrow \mathrm{N}_{\widehat{K}/\mathbf{Q}}(\xi)$. If $q$ is not prime, go to Step (4).
8. Set $\pi \leftarrow N_\Psi(\xi)$. If $q$ is not unramified in $K$, or $\pi$ does not generate $K$, go to Step (4).
9. Return $q$ and $\pi$.

---

**Remark 2.13.** We require $g \geq 2$ in Algorithm 2.12, as the case $g = 1$ is already covered by Example 2.3, and requires a slight adaptation.

The condition that $r$ be prime is for simplicity of presentation only; the algorithm easily extends to square-free values of $r$ that are given as products of splitting primes. Such $r$ are required, for example, by the cryptosystem of [6].

# 3 Performance of the algorithm

**Theorem 3.1.** *If the field $K$ is fixed, then the heuristic expected run time of Algorithm 2.12 is polynomial in* $\log r$.

*Proof.* The algorithm consists of a precomputation for the field $K$ in Steps (1)–(3), followed by a loop in Steps (4)–(7) that is performed until an element $\xi$ is found that has prime norm $N_{\widehat{K}/\mathbf{Q}}(\xi) = q$, and we also find in Step (8) that $q$ is unramified in $K$ and the type norm $\pi = N_\Psi(\xi)$ generates $K$.

The primality condition in Step (7) is the 'true' condition that becomes harder to achieve with increasing $r$, whereas the conditions in Step (8), which are necessary to guarantee correctness of the output, are so extremely likely to be fulfilled (especially in cryptographic applications where $K$ is small and $r$ is large) that they will hardly ever fail in practice and only influence the run time by a constant factor.

As $\xi$ is computed in Step (6) as the lift to $\mathcal{O}_{\widehat{K}}$ of an element $\overline{\xi} \in \mathcal{O}_{\widehat{K}}/r\mathcal{O}_{\widehat{K}} \cong (\mathbf{F}_r)^{2\widehat{g}}$, its norm can be bounded by a constant multiple of $r^{2\widehat{g}}$. Heuristically, $q = \mathrm{N}_{\widehat{K}/\mathbf{Q}}(\xi)$ behaves as a random number, so by the prime number theorem it will be prime with probability at least $(2\widehat{g}\log r)^{-1}$, and we expect that we need to repeat the loop in Steps (4)–(7) about $2\widehat{g}\log r$ times before finding $\xi$ of prime norm $q$. As each of the steps is polynomial in $\log r$, so is the expected run time up to Step (7), and we are done if we show that the conditions in Step (8) are met with some positive probability if $K$ is fixed and $r$ is sufficiently large.

For $q$ being unramified in $K$, one simply notes that only finitely many primes ramify in the field $K$ (which is fixed) and that $q$ tends to infinity with $r$, since $r$ divides $\mathrm{N}_{K/\mathbf{Q}}(\pi - 1) \le (\sqrt{q}+1)^{2g}$.

Finally, we show that $\pi$ generates $K$ with probability tending to 1 as $r$ tends to infinity. Suppose that for every vector $v \in \{0,1\}^{\widehat{g}}$ that is not all 0 or 1, we have

$$\prod_{i=1}^{\widehat{g}} (\alpha_i/\beta_i)^{v_i} \neq 1. \tag{3.2}$$

This set of $2^{\widehat{g}} - 2$ (dependent) conditions on the $2\widehat{g} - 2$ independent random variables $\alpha_i, \beta_i$ for $1 \le i < \widehat{g}$ is satisfied with probability at least $1 - (2^{\widehat{g}} - 2)/(r-1)$. For any automorphism $\phi$ of $L$, the set $\phi \circ \Psi$ is a CM-type of $\widehat{K}$ and there is a $v \in \{0,1\}^{\widehat{g}}$ such that $v_i = 0$ if $\phi \circ \Psi$ contains $\psi_i$ and $v_i = 1$ otherwise. Then $\alpha_i$ is $(\psi_i(\xi) \bmod \mathfrak{R})$, while $\beta_i$ is $(\overline{\psi_i(\xi)} \bmod \mathfrak{R})$, so $(\pi/\phi(\pi) \bmod \mathfrak{R})$ is $\prod_{i=1}^{\widehat{g}} (\alpha_i/\beta_i)^{v_i}$. By (3.2), if this expression is 1 then $v = 0$ or $v = 1$, so $\phi \circ \Psi = \Psi$ or $\overline{\phi} \circ \Psi = \Psi$, which by definition of the reflex is equivalent to $\phi$ or $\overline{\phi}$ being trivial on $K$, i.e., to $\phi$ being trivial on the maximal real subfield $K_0$. Thus if (3.2) holds, then $\phi(\pi) = \pi$ implies that $\phi$ is trivial on $K_0$, hence $K_0 \subset \mathbf{Q}(\pi)$. Since $\pi \in K$ is not real (otherwise, $q = \pi^2$ ramifies in $K$), this implies that $K = \mathbf{Q}(\pi)$. □

In order to maximize the likelihood of finding prime norms, one should minimize the norm of the lift $\xi$ computed in the Chinese Remainder Step (6). This involves minimizing a norm function of degree $2\widehat{g}$ in $2\widehat{g}$ integral variables, which is already infeasible for $\widehat{g} = 2$.

In practice, for given $r$, one lifts a standard basis of $\mathcal{O}_{\widehat{K}}/r\mathcal{O}_{\widehat{K}} \cong (\mathbf{F}_r)^{2\widehat{g}}$ to $\mathcal{O}_{\widehat{K}}$. Multiplying those lifts by integer representatives for the elements $\alpha_i$ and $\beta_i$ of $\mathbf{F}_r$, one quickly obtains lifts $\xi$. We also choose, independently of $r$, a $\mathbf{Z}$-basis of $\mathcal{O}_{\widehat{K}}$ consisting of elements that are 'small' with respect to all absolute values of $\widehat{K}$. We translate $\xi$ by multiples of $r$ to lie in $rF$, where $F$ is the fundamental parallelotope in $\widehat{K} \otimes \mathbf{R}$ consisting of those elements that have coordinates in $(-\frac{1}{2}, \frac{1}{2}]$ with respect to our chosen basis.

If we denote the maximum on $F \cap \widehat{K}$ of all complex absolute values of $\widehat{K}$ by $M_{\widehat{K}}$, we have $q = N_{\widehat{K}/\mathbf{Q}}(\xi) \leq (rM_{\widehat{K}})^{2\widehat{g}}$. For the $\rho$-value (1.1) we find

$$\rho \leq 2g\widehat{g}(1 + \log M_{\widehat{K}}/\log r), \tag{3.3}$$

which is approximately $2g\widehat{g}$ if $r$ gets large with respect to $M_{\widehat{K}}$. We would like $\rho$ to be small, but this is not what one obtains by lifting random admissible choices of $\overline{\xi}$.

**Theorem 3.4.** *If the field $K$ is fixed and $r$ is large, we expect that (1) the output $q$ of Algorithm 2.12 yields $\rho \approx 2g\widehat{g}$, and (2) an optimal choice of $\xi \in \mathcal{O}_{\widehat{K}}$ satisfying the conditions of Theorem 2.10 yields $\rho \approx 2g$.*

**Open problem 3.5.** Find an efficient algorithm to compute an element $\xi \in \mathcal{O}_{\widehat{K}}$ satisfying the conditions of Theorem 2.10 for which $\rho \approx 2g$.

We will prove Theorem 3.4 via a series of lemmas. Let $H_{r,k}$ be the subset of the parallelotope $rF \subset \widehat{K} \otimes \mathbf{R}$ consisting of those $\xi \in rF \cap \mathcal{O}_{\widehat{K}}$ that satisfy the two congruence conditions (2.11) for a given embedding degree $k$. Heuristically, we will treat the elements of $H_{r,k}$ as random elements of $rF$ with respect to the distributions of complex absolute values and norm functions. We will also use the fact that, as $\widehat{K}$ is totally complex of degree $2\widehat{g}$, the $\mathbf{R}$-algebra $\widehat{K} \otimes \mathbf{R}$ is naturally isomorphic to $\mathbf{C}^{\widehat{g}}$. We assume throughout that $g \geq 2$.

**Lemma 3.6.** *Fix the field $K$. Under our heuristic assumption, there exists a constant $c_1 > 0$ such that for all $\varepsilon > 0$, the probability that a random $\xi \in H_{r,k}$ satisfies $q < r^{2(\widehat{g}-\varepsilon)}$ is less than $c_1 r^{-\varepsilon}$.*

*Proof.* The probability that a random $\xi$ lies in the set $V = \{z \in \mathbf{C}^{\widehat{g}} : \prod |z_i|^2 \leq r^{2(\widehat{g}-\varepsilon)}\} \cap rF$ is the quotient of the volume of $V$ by the volume $2^{-\widehat{g}}\sqrt{|\Delta_{\widehat{K}}|}r^{2\widehat{g}}$ of $rF$, where $\Delta_{\widehat{K}}$ is the discriminant of $\widehat{K}$. Now $V$ is contained inside $W = \{z \in \mathbf{C}^{\widehat{g}} : \prod |z_i|^2 \leq r^{2(\widehat{g}-\varepsilon)}, |z_i| \leq rM_{\widehat{K}}\}$, which

has volume

$$(2\pi)^{\widehat{g}} \int_{\substack{x\in[0,rM_{\widehat{K}}]^{\widehat{g}} \\ \prod|x_i|^2\le r^{2(\widehat{g}-\varepsilon)}}} \prod |x_i| dx \quad < \quad (2\pi)^{\widehat{g}} \int_{x\in[0,rM_{\widehat{K}}]^{\widehat{g}}} r^{\widehat{g}-\varepsilon} dx \quad = \quad (2\pi M_{\widehat{K}})^{\widehat{g}} r^{2\widehat{g}-\varepsilon},$$

so a random $\xi$ lies in $V$ with probability less than

$$(4\pi M_{\widehat{K}})^{\widehat{g}} \left|\Delta_{\widehat{K}}\right|^{-1/2} r^{-\varepsilon}. \qquad \square$$

**Lemma 3.7.** *There exists a number $Q_{\widehat{K}}$, depending only on $\widehat{K}$, such that for any positive real number $X < rQ_{\widehat{K}}$, the expected number of $\xi \in H_{r,k}$ with all absolute values below $X$ is*

$$\frac{\varphi(k)(2\pi)^{\widehat{g}}}{\left|\Delta_{\widehat{K}}\right|} \frac{X^{2\widehat{g}}}{r^2}.$$

*Proof.* Let $Q_{\widehat{K}} > 0$ be a lower bound on $\widehat{K} \setminus F$ for the maximum of all complex absolute values, so the box $V_X \subset \widehat{K} \otimes \mathbf{R}$ consisting of those elements that have all absolute values below $X$ lies completely inside $(X/Q_{\widehat{K}})F \subset rF$. The volume of $V_X$ in $\widehat{K} \otimes \mathbf{R}$ is $(\pi X^2)^{\widehat{g}}$, while $rF$ has volume $2^{-\widehat{g}}\sqrt{\left|\Delta_{\widehat{K}}\right|} r^{2\widehat{g}}$. The expected number of $\xi \in H_{r,k}$ satisfying $|\xi| < X$ for all absolute values is $\#H_{r,k} = r^{2\widehat{g}-2}\varphi(k)$ times the quotient of these volumes. $\square$

**Lemma 3.8.** *Fix the field $K$. Under our heuristic assumption, there exists a constant $c_2$ such that for all positive $\varepsilon < 2\widehat{g}-2$, if $r$ is sufficiently large, then we expect the number of $\xi \in H_{r,k}$ satisfying $N_{\widehat{K}/\mathbf{Q}}(\xi) < r^{2+\varepsilon}$ to be at least $c_2 r^{\varepsilon}$.*

*Proof.* Any $\xi$ as in Lemma 3.7 satisfies $N_{\widehat{K}/\mathbf{Q}}(\xi) < X^{2\widehat{g}}$, so we apply the lemma to $X = r^{(1/\widehat{g}+\varepsilon/2\widehat{g})}$, which is less than $rQ_{\widehat{K}}$ for large enough $r$ and $\epsilon < 2\widehat{g} - 2$. $\square$

**Lemma 3.9.** *Fix the field $K$. Under our heuristic assumption, for all $\varepsilon > 0$, if $r$ is large enough, we expect there to be no $\xi \in H_{r,k}$ satisfying $N_{\widehat{K}/\mathbf{Q}}(\xi) < r^{2-\varepsilon}$.*

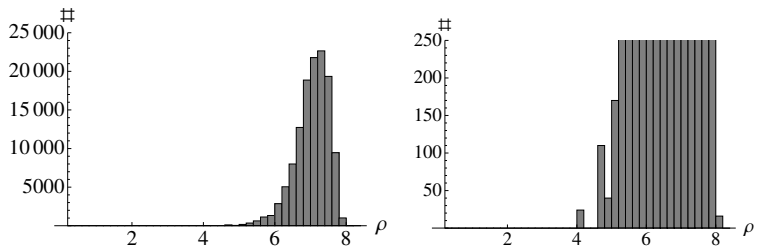
*Proof.* Let $\widehat{\mathcal{O}}$ be the ring of integers of the maximal real subfield of $\widehat{K}$. Let $U$ be the subgroup of norm one elements of $\widehat{\mathcal{O}}^*$. We embed $U$ into $\mathbf{R}^{\widehat{g}}$ by mapping $u \in U$ to the vector $l(u)$ of logarithms of absolute values of $u$. The image is a complete lattice in the $(\widehat{g}-1)$-dimensional

space of vectors with coordinate sum 0. Fix a fundamental parallelotope $F'$ for this lattice. Let $\xi_0$ be the element of $H_{r,k}$ of smallest norm. Since the conditions (2.11), as well as the norm of $\xi_0$, are invariant under multiplication by elements of $U$, we may assume without loss of generality that $l(\xi_0)$ is inside $F' + \mathbf{C}(1, \ldots, 1)$. Then every difference of two entries of $l(\xi_0)$ is bounded, and hence every quotient of absolute values of $\xi_0$ is bounded from below by a positive constant $c_3$ depending only on $K$. In particular, if $m$ is the maximum of all absolute values of $\xi_0$, then $N_{\widehat{K}/\mathbf{Q}}(\xi) > (c_3 m)^{2\widehat{g}}$. Now suppose $\xi_0$ has norm below $r^{2-\varepsilon}$. Then all absolute values of $\xi_0$ are below $X = r^{(1/\widehat{g}-\varepsilon/2\widehat{g})}/c_3$, and $X < rQ_{\widehat{K}}$ for $r$ sufficiently large. Now Lemma 3.7 implies that the expected number of $\xi \in H_{r,k}$ with all absolute values below $X$ is a constant times $r^{-\varepsilon}$, so for any sufficiently large $r$ we expect there to be no such $\xi$, a contradiction. □

*Proof of Theorem 3.4.* The upper bound $\rho \lesssim 2g\widehat{g}$ follows from (3.3). Lemma 3.6 shows that for any $\varepsilon > 0$, the probability that $\rho$ is smaller than $2g\widehat{g} - \varepsilon$ tends to zero as $r$ tends to infinity, thus proving the lower bound $\rho \gtrsim 2g\widehat{g}$. Lemma 3.8 shows that for any $\varepsilon > 0$, if $r$ is sufficiently large then we expect there to exist a $\xi$ with $\rho$-value at most $2g + \varepsilon$, thus proving the bound $\rho \lesssim 2g$. Lemma 3.9 shows that we expect $\rho > 2g - \varepsilon$ for the optimal $\xi$, which proves the bound $\rho \gtrsim 2g$. □

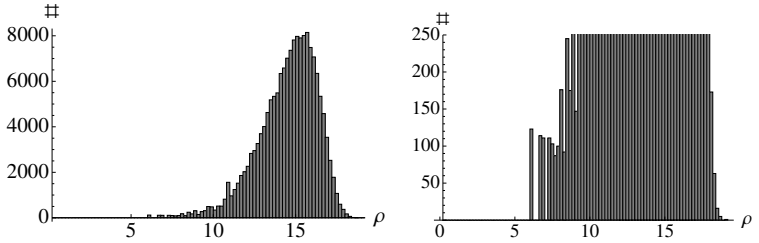
For very small values of $r$ we are able to do a brute-force search for the smallest $q$ by testing all possible values of $\alpha_1, \ldots, \alpha_{\widehat{g}-1}, \beta_1, \ldots, \beta_{\widehat{g}-1}$ in Step 4 of Algorithm 2.12. We performed two such searches, one in dimension 2 and one in dimension 3. The experimental results support our heuristic evidence that $\rho \approx 2g$ is possible with a smart choice in the algorithm, and that $\rho \approx 2g\widehat{g}$ is achieved with a randomized algorithm.

**Example 3.10.** Take $K = \mathbf{Q}(\zeta_5)$, and let $\Phi = \{\phi_1, \phi_2\}$ be the CM-type of $K$ defined by $\phi_n(\zeta_5) = e^{2\pi i n/5}$. We ran Algorithm 2.12 with $r = 1021$ and $k = 2$, and tested all possible values of $\alpha_1, \beta_1$. The total number of primes $q$ found was 125578, and the corresponding $\rho$-values were distributed as follows:



The smallest $q$ found was 2023621, giving a $\rho$-value of 4.19. The curve over $\mathbf{F} = \mathbf{F}_q$ for which the Jacobian has this $\rho$-value is $y^2 = x^5 + 18$, and the number of points on its Jacobian is 4092747290896.

**Example 3.11.** Take $K = \mathbf{Q}(\zeta_7)$, and let $\Phi = \{\phi_1, \phi_2, \phi_3\}$ be the CM-type of $K$ defined by $\phi_i(\zeta_7) = e^{2\pi i/7}$. We ran Algorithm 2.12 with $r = 29$ and $k = 4$, and tested all possible values of $\alpha_1, \alpha_2, \beta_1, \beta_2$. The total number of primes $q$ found was 162643, and the corresponding $\rho$-values were distributed as follows:




The smallest $q$ found was 911, giving a $\rho$-value of 6.07. The curve over $\mathbf{F} = \mathbf{F}_q$ for which the Jacobian has this $\rho$-value is $y^2 = x^7 + 34$, and the number of points on its Jacobian is 778417333.

**Example 3.12.** Take $K = \mathbf{Q}(\zeta_5)$, and let $\Phi = \{\phi_1, \phi_2\}$ be the CM-type of $K$ defined by $\phi_i(\zeta_5) = e^{2\pi i/5}$. We ran Algorithm 2.12 with $r = 2^{160} + 685$ and $k = 10$, and tested $2^{20}$ random values of $\alpha_1, \beta_1$. The total number of primes $q$ found was 7108. Of these primes, 6509 (91.6%) produced $\rho$-values between 7.9 and 8.0, while 592 (8.3%) had $\rho$-values between 7.8 and 7.9. The smallest $q$ found had 623 binary digits, giving a $\rho$-value of 7.78.

# 4 Constructing abelian varieties with given Weil numbers

Our Algorithm 2.12 yields $q$-Weil numbers $\pi \in K$ that correspond, in the sense of Honda and Tate [84], to isogeny classes of ordinary, simple abelian varieties over prime fields that have a point of order $r$ and embedding degree $k$ with respect to $r$. It does not give a method to explicitly construct an abelian variety $A$ with Frobenius $\pi \in K$. In this section we focus on the problem of explicitly constructing such varieties using complex multiplication techniques.

The key point of the complex multiplication construction is the fact that every ordinary, simple abelian variety over $\mathbf{F} = \mathbf{F}_q$ with Frobenius

$\pi \in K$ arises as the reduction at a prime over $q$ of some abelian variety $A_0$ in characteristic zero that has CM by the ring of integers of $K$. Thus if we have fixed our $K$ as in Algorithm 2.12, we can solve the construction problem for all ordinary Weil numbers coming out of the algorithm by compiling the finite list of $\overline{\mathbf{Q}}$-isogeny classes of abelian varieties in characteristic zero having CM by $\mathcal{O}_K$. There will be one $\overline{\mathbf{Q}}$-isogeny class for each equivalence class of primitive CM-types of $K$, where $\Phi$ and $\Phi'$ are said to be equivalent if we have $\Phi = \Phi' \circ \sigma$ for an automorphism $\sigma$ of $K$. As we can choose our favorite field $K$ of degree $2g$ to produce abelian varieties of dimension $g$, we can pick fields $K$ for which such lists already occur in the literature.

From representatives of our list of isogeny classes of abelian varieties in characteristic zero having CM by $\mathcal{O}_K$, we obtain a list $\mathcal{A}$ of abelian varieties over $\mathbf{F}$ with CM by $\mathcal{O}_K$ by reducing at some fixed prime $\mathfrak{q}$ over $q$. Changing the choice of the prime $\mathfrak{q}$ amounts to taking the reduction at $\mathfrak{q}$ of a conjugate abelian variety which also has CM by $\mathcal{O}_K$ and hence is $\overline{\mathbf{F}}$-isogenous to one already in the list.

For every abelian variety $A \in \mathcal{A}$, we compute the set of its twists, i.e., all the varieties up to $\mathbf{F}$-isomorphism that become isomorphic to $A$ over $\overline{\mathbf{F}}$. There is at least one twist $B$ of an element $A \in \mathcal{A}$ satisfying $\#B(\mathbf{F}) = \mathrm{N}_{K/\mathbf{Q}}(\pi - 1)$, and this $B$ has a point of order $r$ and the desired embedding degree.

Note that while efficient point counting algorithms do not exist for varieties of dimension $g > 1$, we can determine probabilistically whether an abelian variety has a given order by choosing a random point, multiplying by the expected order, and seeing if the result is the identity.

The complexity of the construction problem rapidly increases with the genus $g = [K : \mathbf{Q}]/2$, and it is fair to say that we only have satisfactory general methods at our disposal in very small genus.

In genus one, we are dealing with elliptic curves. The $j$-invariants of elliptic curves over $\mathbf{C}$ with CM by $\mathcal{O}_K$ are the roots of the *Hilbert class polynomial* of $K$, which lies in $\mathbf{Z}[X]$. The degree of this polynomial is the class number $h_K$ of $K$, and it can be computed in time $\widetilde{O}(|\Delta_K|)$.

For genus 2, we have to construct abelian surfaces. Any principally polarized simple abelian surface over $\overline{\mathbf{F}}$ is the Jacobian of a genus 2 curve, and all genus 2 curves are hyperelliptic. There is a theory of class polynomials analogous to that for elliptic curves, as well as several algorithms to compute these polynomials, which lie in $\mathbf{Q}[X]$. The genus 2 algorithms are not as well-developed as those for elliptic curves; at present they can handle only very small quartic CM-fields, and there exists no rigorous run time estimate. From the roots in $\mathbf{F}$ of these polynomials, we can compute the genus 2 curves using Mestre's algorithm.

Any three-dimensional principally polarized simple abelian variety over $\overline{\mathbf{F}}$ is the Jacobian of a genus 3 curve. There are two known families of genus 3 curves over $\mathbf{C}$ whose Jacobians have CM by an order of dimension 6. The first family, due to Weng [95], gives hyperelliptic curves whose Jacobians have CM by a degree-6 field containing $\mathbf{Q}(i)$. The second family, due to Koike and Weng [51], gives Picard curves (curves of the form $y^3 = f(x)$ with $\deg f = 4$) whose Jacobians have CM by a degree-6 field containing $\mathbf{Q}(\zeta_3)$.

Explicit CM-theory is mostly undeveloped for dimension $\geq 3$. Moreover, most principally polarized abelian varieties of dimension $\geq 4$ are not Jacobians, as the moduli space of Jacobians has dimension $3g-3$, while the moduli space of abelian varieties has dimension $g(g+1)/2$. For implementation purposes we prefer Jacobians or even hyperelliptic Jacobians, as these are the only abelian varieties for which group operations can be computed efficiently.

In cases where we cannot compute every abelian variety in characteristic zero with CM by $\mathcal{O}_K$, we use a single such variety $A$ and run Algorithm 2.12 for each different CM-type of $K$ until it yields a prime $q$ for which the reduction of $A$ mod $q$ is in the correct isogeny class. An example for $K = \mathbf{Q}(\zeta_{2p})$ with $p$ prime is given by the Jacobian of $y^2 = x^p + a$, which has dimension $g = (p-1)/2$.

# 5 Numerical examples

We implemented Algorithm 2.12 in MAGMA and used it to compute examples of hyperelliptic curves of genus 2 and 3 over fields of cryptographic size for which the Jacobians are pairing-friendly. The subgroup size $r$ is chosen so that the discrete logarithm problem in $A[r]$ is expected to take roughly $2^{80}$ steps. The embedding degree $k$ is chosen so that $r^{k/g} \approx 1024$; this would be the ideal embedding degree for the 80-bit security level if we could construct varieties with $\#A(\mathbf{F}) \approx r$. Space constraints prevent us from giving the group orders for each Jacobian, but we note that a set of all possible $q$-Weil numbers in $K$, and hence all possible group orders, can be computed from the factorization of $q$ in $K$.

**Example 5.1.** Let $\eta = \sqrt{-2+\sqrt{2}}$ and let $K$ be the degree-4 Galois CM-field $\mathbf{Q}(\eta)$. Let $\Phi = \{\phi_1, \phi_2\}$ be the CM-type of $K$ such that $\mathrm{Im}(\phi_i(\eta)) > 0$. We ran Algorithm 2.12 with CM-type $(K, \Phi)$, $r = 2^{160} - 1679$, and $k = 13$. The algorithm output the following field size:

$q = 31346057808293157913762344531005275715544680219641338497449500238872\backslash$
$30035061716540892530853973205578151445285706963588204818794198739264\backslash$
$12384900210489039945980746313273247715465151766675570216 7$ (640 bits)

There is a single $\overline{\mathbf{F}}_q$-isomorphism class of curves over $\mathbf{F}_q$ whose Jacobians have CM by $\mathcal{O}_K$ and it has been computed in [88]; the desired twist turns out to be $C : y^2 = -x^5 + 3x^4 + 2x^3 - 6x^2 - 3x + 1$. The $\rho$-value of $\mathrm{Jac}(C)$ is 7.99.

**Example 5.2.** Let $\eta = \sqrt{-30 + 2\sqrt{5}}$ and let $K$ be the degree-4 non-Galois CM field $\mathbf{Q}(\eta)$. The reflex field $\widehat{K}$ is $\mathbf{Q}(\omega)$ where

$$\omega = \sqrt{-15 + 2\sqrt{55}}.$$

Let $\Psi$ be the CM-type of $K$ such that $\mathrm{Im}(\phi_i(\eta)) > 0$. We ran Algorithm 2.12 with the CM-type $(K, \Phi)$, subgroup size $r = 2^{160} - 1445$, and embedding degree $k = 13$. The algorithm output the following field size:

$q = 11091654887169512971365407040293599579976378158973405181635081379157\backslash$
$07830213092751652003623786192531077127388944453303584091334492452752\backslash$
$69309408919298654153381935518866167783400231181308345981461$ (645 bits)

The class polynomials for $K$ can be found in the preprint version of [97]. We used the roots of the class polynomials mod $q$ to construct curves over $\mathbf{F}_q$ with CM by $\mathcal{O}_K$. As $K$ is non-Galois with class number 4, there are 8 isomorphism classes of curves in 2 isogeny classes. We found a curve $C$ in the correct isogeny class with equation $y^2 = x^5 + a_3x^3 + a_2x^2 + a_1x + a_0$, with

$a_3 = 37909827361040902434390338072754918705969566622865244598340785379492\backslash$
$06229349302307887220632471591953460261515915189503199574055791975955\backslash$
$83440787957848421270026326004014371084570321085865481897 69$
$a_2 = 18960350992731066141619447121681062843951822341216980089632110294900\backslash$
$98526734892756700435114431697785479098782721806327279074708206429263\backslash$
$75198310935125083185373519012820004210701825726715060564 32$
$a_1 = 69337488142924022910219499907432470174331183248226721112535199929650\backslash$
$66326048728150177351432967251207037416196614255668796808046612641767\backslash$
$92227374912536654153444058824657313765233049070410064645 04$
$a_0 = 31678142561939596895646021753607012342277658384169880961095701825776\backslash$
$70412620481848230687778916790603969757571449880417861689471274167016\backslash$
$38860871296694117812042438133326172720384940201785611195 64.$

The $\rho$-value of $\mathrm{Jac}(C)$ is 8.06.

**Example 5.3.** Let $K$ be the degree-6 Galois CM-field $\mathbf{Q}(\zeta_7)$, and let $\Phi = \{\phi_1, \phi_2, \phi_3\}$ be the CM type of $K$ such that $\phi_n(\zeta_7) = e^{2\pi i n/7}$. We used the CM-type $(K, \Phi)$ to construct a curve $C$ whose Jacobian has embedding degree 17 with respect to $r = 2^{180} - 7427$. Since $K$ has class number 1 and one equivalence class of primitive CM-types, there is a unique isomorphism class of curves in characteristic zero whose Jacobians are simple and have CM by $K$; these curves are given by $y^2 = x^7 + a$. Algorithm 2.12 output the following field size:

$$\begin{aligned} q = {} & 157558413811977153591787802014368793057776946867137463955067876140 25\backslash \\ & 008121759749726349377162542168169176007186988081292604570406371468 02\backslash \\ & 812702044068612772692590771889662051561078068230000961208749156120 17\backslash \\ & 184924206843204621759232946263357637192516979877402638911689714410 85\backslash \\ & 531481109276328740299111531260484082698571214310334 99 \quad (1077 \text{ bits}) \end{aligned}$$

The equation of the curve $C$ is $y^2 = x^7 + 10$. The $\rho$-value of $\mathrm{Jac}(C)$ is 17.95.

We conclude with an example of an 8-dimensional abelian variety found using our algorithms. We started with a single CM abelian variety $A$ in characteristic zero and applied our algorithm to different CM-types until we found a prime $q$ for which the reduction has the given embedding degree.

**Example 5.4.** Let $K = \mathbf{Q}(\zeta_{17})$. We set $r = 1021$ and $k = 10$ and ran Algorithm 2.12 repeatedly with different CM-types[1] for $K$. Given the output, we tested the Jacobians of twists of $y^2 = x^{17} + 1$ for the specified number of points. We found that the curve $y^2 = x^{17} + 30$ has embedding degree 10 with respect to $r$ over the field $\mathbf{F}$ of order

$$q = 68696035083224346148549085355452089780388194 37.$$

The CM-type was

$$\Phi = \{\phi_1, \phi_3, \phi_5, \phi_6, \phi_8, \phi_{10}, \phi_{13}, \phi_{15}\},$$

where $\phi_n(\zeta_{17}) = e^{2\pi i n/17}$. The $\rho$-value of $\mathrm{Jac}(C)$ is 121.9.

[1] Originally, we tried different random CM-types until it worked. The CM-type $\Phi$ written in the example turned out to work. Actually, we could have predicted this correct CM-type. See Example III.4.5.

Chapter V

# Abelian surfaces with $p$-rank 1

This chapter appeared before up to minor corrections as Laura Hitt O'Connor, Gary McGuire, Michael Naehrig, and Marco Streng, *A CM construction for curves of genus* 2 *with p-rank* 1, arXiv:0811.3434v2 [43]. The final published form may differ from this version.

ABSTRACT. *We construct Weil numbers corresponding to genus-*2 *curves with p-rank* 1 *over the finite field* $\mathbf{F}_{p^2}$ *of* $p^2$ *elements. The corresponding curves can be constructed using explicit CM constructions. In one of our algorithms, the group of* $\mathbf{F}_{p^2}$*-valued points of the Jacobian has prime order, while another allows for a prescribed embedding degree with respect to a subgroup of prescribed order. The curves are defined over* $\mathbf{F}_{p^2}$ *out of necessity: we show that curves of p-rank* 1 *over* $\mathbf{F}_p$ *for large p cannot be efficiently constructed using explicit CM constructions.*

## 1 Introduction

The *p-rank* of an abelian variety $A$ over a field $k$ of characteristic $p$ is the integer $r = r(A)$ such that the group $A[p](\overline{k})$ of $p$-torsion points over an algebraic closure $\overline{k}$ of $k$ has order $p^r$. It satisfies $0 \leq r \leq g$, where $g$ is the dimension of $A$, and we call $A$ *ordinary* if $r$ is equal to $g$. If

$A$ is *supersingular*, that is, if $A$ becomes isogenous over $\overline{k}$ to a product of supersingular elliptic curves, then we have $r = 0$, and the converse holds for abelian surfaces: if $r = 0$ and $g = 2$, then $A$ is supersingular.

This shows that for an abelian surface $A$, besides the ordinary and supersingular cases, there is only one *intermediate* case: the case where $A$ has $p$-rank 1. Most CM constructions of curves of genus two [79, 97, 24, 26] generate curves that are ordinary with probability tending to 1, while another [69] constructs only supersingular curves. We focus on the intermediate case, for which no constructions existed yet.

The $p$-rank $r(A)$ depends only on the *isogeny class* of $A$ over $\overline{k}$, and any simple abelian surface $A$ of $p$-rank 1 over a finite field $k$ is isogenous to the Jacobian of a curve over $k$ of genus 2 (see Section 2). By the $p$-rank of a curve $C$, we mean the $p$-rank of its Jacobian $J_C$.

Let $k$ be the finite field of order $q = p^n$. The Frobenius endomorphism $\pi$ of a simple abelian variety over $k$ is a *Weil $q$-number*, i.e., an algebraic integer $\pi$ such that $|\pi|^2 = q$ holds for every embedding of the field $K = \mathbf{Q}(\pi)$ into the complex numbers. A theorem of Honda and Tate [84] states that this defines a bijection between the set of isogeny classes of simple abelian varieties over $k$ and the set of Weil $q$-numbers up to Galois conjugacy.

We characterize those Weil numbers corresponding to abelian surfaces with $p$-rank 1 in Section 2, show their existence in Section 3 and give algorithms for finding them in Section 4. In Section 3 we also explain why curves of $p$-rank 1 over $\mathbf{F}_p$ for large $p$ cannot be efficiently constructed using explicit CM constructions.

The construction of an abelian variety $A$ corresponding to a given Weil $q$-number $\pi$ dates back to Shimura and Taniyama [78] and Honda [44]. It exhibits $A$ as the reduction of a characteristic-0 abelian variety with *complex multiplication (CM)* by $\mathbf{Z}[\pi]$ and is also known as the *CM method*. We explain this explicit CM construction in Section 5. For now, it suffices to say that the computational complexity of this construction grows very rapidly with the size of the field $K = \mathbf{Q}(\pi)$. Therefore, our algorithms will look for Weil $q$-numbers $\pi$ only in fixed small input fields $K$.

Let $A$ be an abelian variety over the finite field $k$ and suppose that $A(k)$ has a subgroup of prime order $r$. The *embedding degree* of $A$ with respect to $r$ is the degree of the field extension $k(\zeta_r)/k$, where $\zeta_r$ is a primitive $r$-th root of unity. The *Weil* and *Tate* pairings on $A$ with respect to $r$ have their image in $\langle\zeta_r\rangle \subset k(\zeta_r)^*$, and in order to compute these pairings, one needs to work with $k(\zeta_r)$. As the embedding degree is the order of $q$ in $(\mathbf{Z}/r\mathbf{Z})^*$, it is close to $r$ for most curves, while for *pairing-based cryptography*, one wants $r$ to be large and the embedding

degree to be small. Algorithm 3 in Section 4 provides curves with $p$-rank 1 and a prescribed small embedding degree.

We used our algorithms to compute various examples, which we give in Section 8. Each example was computed in a few seconds on a standard PC.

## 2 Characterization of abelian surfaces with $p$-rank one

It follows from the definition that the $p$-rank $r(A)$ of an abelian variety $A$ does not change under extensions of the base field, and that it satisfies $r(A \times B) = r(A) + r(B)$ for any pair of abelian varieties $A$ and $B$. It is also well-known that the $p$-rank is invariant under isogeny (see Lemma 2 below). In particular, the non-simple abelian surfaces of $p$-rank 1 are exactly those isogenous to the product of an ordinary and a supersingular elliptic curve. Both types of elliptic curves are well understood, so we focus on *simple* abelian surfaces. We use the word *isogeny* to mean isogeny defined over the base field $k$, unless otherwise stated. We use the same convention for the definition of *simple* abelian variety.

Our algorithms are based on a characterization of Weil numbers corresponding to simple abelian surfaces of $p$-rank 1, which we give in this section. A major part of this characterization can already be found in Goren [34] and Gonzalez [33, proof of Thm. 3.7], but we give a proof, as this result is the foundation of our construction.

Let $k$ be the finite field of $q = p^n$ elements and let $\pi$ be a Weil $q$-number. For every embedding of the field $K = \mathbf{Q}(\pi)$ into $\mathbf{C}$, complex conjugation on $K$ is given by $\pi \mapsto q/\pi$. As this automorphism of $K$ doesn't depend on the choice of the embedding, we denote it by $x \mapsto \overline{x}$ and call it complex conjugation. If we let $K_0$ be the fixed field of complex conjugation, then $K_0$ is totally real and $K$ is either equal to $K_0$ or it is a *CM-field*, that is, a totally imaginary quadratic extension of a totally real number field.

**Lemma 1.** *A simple abelian variety $A$ over the field $k$ of $q = p^n$ elements has dimension 2 and $p$-rank 1 if and only if the following three conditions hold for its Frobenius endomorphism $\pi$:*

*(1) the field $K = \mathbf{Q}(\pi)$ is a CM-field of degree 4,*

*(2) the prime $p$ factors in $K$ as $p\mathcal{O}_K = \mathfrak{p}_1\overline{\mathfrak{p}_1}\mathfrak{p}_2^e$, with $e \in \{1, 2\}$, and*

*(3) we have $\pi\mathcal{O}_K = \mathfrak{p}_1^n\mathfrak{p}_2^{en/2}$ with $e$ as in (2).*

*Note that condition (3) implies that $en$ is even.*

We prove Lemma 1 using the following formula for the $p$-rank of an abelian variety.

**Lemma 2** ([33, Prop. 3.1])**.** *Let $A$ be a simple abelian variety over $k$ and let $K = \mathbf{Q}(\pi)$, where $\pi$ is the Frobenius endomorphism of $A$. There is an integer $m$ such that $2\dim(A) = m \deg K$ holds. Suppose that $p$ factors in $K$ as $p\mathcal{O}_K = \prod_i \mathfrak{p}_i^{e_i}$ and let $f_i$ be given by $\#(\mathcal{O}_K/\mathfrak{p}_i) = p^{f_i}$. Then we have $r(A) = \sum m e_i f_i$, where the sum is taken over those $i$ for which $\pi \notin \mathfrak{p}_i$ holds.*

*Proof.* The *degree* $\deg g$ and *separable degree* $\deg_{\mathrm{s}} g$ of an isogeny $g : A \to B$ of abelian varieties are defined to be the degree and separable degree of the induced embedding of function fields $g^* : k(B) \to k(A)$. We have $\#(\ker g)(\overline{k}) = \deg_{\mathrm{s}} g$, hence $p^{r(A)}$ is the separable degree of the multiplication-by-$p$ map on $A$. As the separable degree is multiplicative under composition, we find that the $p$-rank of $A$ depends only on its isogeny class, hence we can assume that $\mathrm{End}_k A$ contains the maximal order $\mathcal{O}_K$ by [78, Prop. 7 in §7.1].

The existence of $m$ follows from [84, Thm. 1(2)]. The theory in [78, §7] shows how to factor the multiplication-by-$p$ map into multiplication-by-$\mathfrak{p}_i$ maps for prime ideals $\mathfrak{p}_i$, and that the multiplication-by-$\mathfrak{p}_i$ map has degree $p^{f_i m}$. The Frobenius endomorphism $\pi$ is totally inseparable by [78, Thm. 1(iii) in §2.8], hence so is multiplication-by-$\mathfrak{p}_i$ if $\mathfrak{p}_i$ contains $\pi$. If $\mathfrak{p}_i$ is coprime to $\pi$, then [78, Prop. 6 in §2.8] shows that it is separable, hence satisfies $\deg_{\mathrm{s}} \mathfrak{p}_i = \deg \mathfrak{p}_i$. □

*Proof of Lemma 1.* If $A$ has dimension 2 and $p$-rank 1, then Lemma 2 tells us $m = 1$, hence $K$ has degree 4 and exactly one prime $\overline{\mathfrak{p}_1}|p$ with $\pi \notin \overline{\mathfrak{p}_1}$, which is unramified and has residue degree 1. This implies $p\mathcal{O}_K = \mathfrak{p}_1\overline{\mathfrak{p}_1}\mathfrak{q}$, where $\mathfrak{q}$ is prime in the fixed field $K_0$ of complex conjugation.

To prove that (2) and (3) hold, it now suffices to prove that $\mathfrak{q}$ does not split in $K/K_0$. Suppose that it does, say $\mathfrak{q} = \mathfrak{q}_1\overline{\mathfrak{q}_1}$. Then by [84, Thm. 1(1)], the fact $m = 1$ implies that $\mathrm{ord}_{\mathfrak{q}_1}(\pi)$ is either 0 or equal to the degree $n = \deg k/\mathbf{F}_p$. We also have $\mathrm{ord}_{\mathfrak{q}_1}(\pi) + \mathrm{ord}_{\overline{\mathfrak{q}_1}}(\pi) = \mathrm{ord}_{\mathfrak{q}_1}(\pi\overline{\pi}) = n$, hence one of $\mathfrak{q}_1$ and $\overline{\mathfrak{q}_1}$ does not divide $\pi$, i.e., contradicts uniqueness of $\overline{\mathfrak{p}_1}$.

Conversely, if $\pi$ satisfies (1), (2), and (3), then Lemma 2 implies $r(A) = m$ with $2\dim(A) = m \deg K$ and [84, Thm. 1(1)] implies $m = 1$. □

**Corollary 3.** A simple abelian surface $A/k$ of $p$-rank 1 is absolutely simple, that is, simple over $\overline{k}$, and is isogenous to the Jacobian of a curve $C$ over $k$.

*Proof.* Suppose that $k'/k$ is an extension of degree $d$ such that we have $A_{k'} \sim E \times F$. The Frobenius endomorphism of $A_{k'}$ is $\pi^d$ and the characteristic polynomial of its action on the $\ell$-adic Tate module of $A$ for $l \neq p$ is the product of the (quadratic) characteristic polynomials of the action on the Tate modules of $E$ and $F$.

On the other hand, part (3) of Lemma 1 implies that $\mathbf{Q}(\pi^d)$ is equal to $K$, which is a field of degree 4. This is a contradiction, hence $A$ is absolutely simple.

By [59, Theorem 4.3], any absolutely simple abelian surface over a finite field $k$ is isogenous to the Jacobian of a curve. □

**Remark 4.** The conditions (1), (2), and (3) of Lemma 1 are equivalent to conditions (M) of Theorem 2.9 of Maisner and Nart [59], i.e., to the characteristic polynomial $f = X^4 - a_1X^3 + (a_2 + 2q)X^2 - qa_1X + q^2$ of $\pi$ satisfying

(1) $f$ is irreducible,

(2) $\mathrm{ord}_p(a_1) = 0$,

(3) $\mathrm{ord}_p(a_2) \geq n/2$,

(4) and that $(a_2 + 4q)^2 - 4qa_1^2$ is not a square in the ring of $p$-adic integers $\mathbf{Z}_p$.

**Remark 5.** For an elliptic curve $E$ over a finite field $k$, the rank of the $\mathbf{Z}$-algebra $\mathrm{End}_{\overline{k}}(E)$ of $\overline{k}$-endomorphisms is either 2 or 4, and these cases correspond exactly to the cases $r(E) = 1$ and $r(E) = 0$.

For abelian surfaces $A$, the $p$-rank $r(A)$ cannot be computed from the $\mathbf{Z}$-rank of the endomorphism algebra. In fact, for absolutely simple abelian surfaces $A$, the ring $\mathrm{End}_{\overline{k}}(A) \otimes \mathbf{Q}$ is always a CM-field of degree 4, while both $r(A) = 1$ and $r(A) = 2$ occur (see also [33, Thm 3.7(ii)]).

# 3 Existence of suitable Weil numbers

Let $p$ be a prime that factors in $K$ as in (2) of Lemma 1. The fact that not all primes over $p$ have the same ramification index or residue degree implies that the degree-4 extension $K/\mathbf{Q}$ is not Galois. As $K$ has a non-trivial automorphism, complex conjugation, the normal closure $L$ of $K$ has Galois group $D_4$. We therefore have to restrict to non-Galois quartic number fields $K$ with Galois group $D_4$.

In the case $e = 2$, the prime $p$ ramifies in $K$, hence divides its discriminant. Since explicit CM constructions are feasible only for small fields $K$, i.e., fields $K$ of small discriminant, this means that we can construct the curve $C$ corresponding to $\pi$ only for very small values

of $p$. For such small values of $p$, not only are the curves less interesting, especially from a cryptographic point of view, it also becomes possible to construct them using a more direct approach such as by enumerating all curves $C$ of genus 2 over $\mathbf{F}_p$ and computing the group orders of their Jacobians. Therefore, we will focus on the case $e = 1$. For $e = 1$, condition (3) of Lemma 1 implies $2|n$, so that curves are defined only over fields containing $\mathbf{F}_{p^2}$. This is the reason why we construct our curves over $\mathbf{F}_{p^2}$ and not over $\mathbf{F}_p$, and this is why curves of $p$-rank 1 over $\mathbf{F}_p$ for large $p$ cannot be efficiently constructed using explicit CM constructions.

We have found that all fields with $p$-rank-1 Weil $p^2$-numbers are quartic non-Galois CM-fields. However, not all quartic non-Galois CM-fields have $p$-rank-1 Weil $p^2$-numbers, and we give a complete characterization in Section 6.

For now, we give two lemmas that put a condition on the CM-fields $K$ that is slightly too strong, but is easy to check and is satisfied by 'most' non-Galois quartic CM-fields.

**Lemma 6.** *Let $K$ be a quartic CM-field and let $p$ be a prime that factors in $K$ as $p\mathcal{O}_K = \mathfrak{p}_1\overline{\mathfrak{p}_1}\mathfrak{p}_2$. Suppose that $\mathfrak{p}_1 = \alpha\mathcal{O}_K$ is principal. Then $\pi = \alpha\overline{\alpha}^{-1}p$ is a Weil $p^2$-number that satisfies the conditions of Lemma 1.*

*Proof.* The number $\pi$ satisfies $\pi\overline{\pi} = p^2$, hence is a Weil $p^2$-number. Conditions (1) and (2) of Lemma 1 are satisfied by assumption. Moreover, we have $\mathfrak{p}_2 = p(\mathfrak{p}_1\overline{\mathfrak{p}_1})^{-1} = p(\alpha\overline{\alpha})^{-1}\mathcal{O}_K$, so that we have $\pi\mathcal{O}_K = \mathfrak{p}_1^2\mathfrak{p}_2$, i.e., condition (3) is also satisfied. □

The condition on $p$ of Lemma 6 is stronger than the condition that there exists a Weil $p^2$-number in $K$ with $e = 1$. The following lemma gives a necessary and sufficient criterion on $K$ for the existence of primes $p$ satisfying this stronger condition.

For a non-Galois quartic CM-field $K$, let $L$ be its normal closure over $\mathbf{Q}$ and let $d$ be the discriminant of the real quadratic subfield $K_0$ of $K$. Then we have $K = K_0(\sqrt{r})$ for a totally negative element $r \in K_0$, and $s = N_{K_0/\mathbf{Q}}(r) \in \mathbf{Q}$ is not a square, because $K$ is non-Galois. Let $d^{\mathrm{r}}$ be the discriminant of the real quadratic field $K_0^{\mathrm{r}} = \mathbf{Q}(\sqrt{s})$. Note that this field is independent of the choice of $r$. Indeed, the element $r$ is well-defined up to squares in $K_0^*$, hence $s$ is well-defined up to squares in $\mathbf{Q}^*$.

A *prime discriminant* is a number that is $-4$ or $\pm 8$ or is $\pm p \equiv 1 \pmod 4$ for an odd prime $p$. The discriminant of a quadratic field can be written uniquely as a product of distinct prime discriminants in which at most one even factor occurs.

**Lemma 7.** *Let $K$ be a non-Galois quartic CM-field. The following are equivalent*

*(1) there exists a prime $p$ that factors in $K$ as $p\mathcal{O}_K = \mathfrak{p}_1\overline{\mathfrak{p}_1}\mathfrak{p}_2$ with $\mathfrak{p}_1$ principal;*

*(2) the Dirichlet density of the set of primes $p$ as in (1) is $(4h_K)^{-1}$, where $h_K$ is the class number of $K$;*

*(3) there is a prime that ramifies in $L/K$;*

*(4) not all prime discriminants in the discriminant factorization of $d^{\mathrm{r}}$ occur in that of $d$.*

*Proof.* The implication (2) $\Rightarrow$ (1) is trivial. Now suppose that (1) holds, so the decomposition group of $\mathfrak{p}_1$ in $\mathrm{Gal}(L/\mathbf{Q})$ is $\mathrm{Gal}(L/K)$ and the ideal class of $\mathfrak{p}_1$ is trivial. By the Artin isomorphism $\mathrm{Cl}_K \to \mathrm{Gal}(H/K)$, this implies that the decomposition group of $\mathfrak{p}_1$ in $\mathrm{Gal}(H/K)$ is trivial for the Hilbert class field $H$ of $K$. As the decomposition group of $\mathfrak{p}_1$ in $\mathrm{Gal}(L/K)$ is non-trivial, this implies that $L$ is not contained in the maximal unramified abelian extension $H$ of $K$, so $L/K$ ramifies at some prime and (3) holds.

For the proof of (3) $\Rightarrow$ (2), we use again that the primes $p$ as in (1) are those for which there exists a prime in $L$ over $p$ with decomposition group $\mathrm{Gal}(L/K)$ in $L/\mathbf{Q}$ and trivial decomposition group $H/K$. Let $M \supset H$ be Galois over $\mathbf{Q}$. Since (3) implies $L \cap H = K$, we find $\mathrm{Gal}(HL/K) = \mathrm{Gal}(H/K) \times \mathrm{Gal}(L/K)$ and hence that exactly 1 in every $8h_K$ elements $\sigma \in \mathrm{Gal}(M/\mathbf{Q})$ satisfies $\langle \sigma_{|L} \rangle = \mathrm{Gal}(L/K)$ and $\sigma_{|H} = 1$. The conjugation class of $\mathrm{Gal}(L/K)$ in $\mathrm{Gal}(L/\mathbf{Q})$ has two elements, hence the set of all $\sigma$ yielding the appropriate factorization is twice as large, i.e., consists of 1 in every $4h_K$ elements of $\mathrm{Gal}(M/\mathbf{Q})$. By Chebotarev's density theorem [66, Theorem 13.4], this implies that the density of primes with this factorization is $(4h_K)^{-1}$, which proves (2).

Now, it remains to prove (3) $\Leftrightarrow$ (4). Let $L_0$ be the compositum of $K_0$ and $K_0^{\mathrm{r}}$ in $L$. A prime $q \in \mathbf{Z}$ ramifies in $L/K$ if and only if its inertia group in $\mathrm{Gal}(L/\mathbf{Q})$ contains $\mathrm{Gal}(L/K)$ or its conjugate. This is equivalent to $q$ ramifying in $L_0/K_0$, that is, to the prime discriminant in $d^{\mathrm{r}}$ corresponding to $q$ not occurring in the prime discriminant factorization of $d$. □

**Example 8.** The field $K = \mathbf{Q}[X]/(X^4 + 12X^2 + 2)$ does not satisfy the conditions of Lemma 7, because it has $d = 8 \cdot 17$ and $d^{\mathrm{r}} = 8$.

For 'most' non-Galois quartic CM-fields $K$, the discriminant $d^{\mathrm{r}}$ does not divide $d$, in which case the conditions of Lemma 7 hold. This means that if we try to find our Weil numbers by taking random primes $p$ and

checking if there exists a Weil $p^2$-number $\pi \in K$ as in Lemma 1, then we have a probability $(4h_K)^{-1}$ of success.

# 4 The algorithms

The discussion in Section 3 leads to the following algorithm.

---

**Algorithm 1.**
**Input:** A non-Galois CM-field $K$ of degree 4 and a positive integer $\ell$.
**Output:** A prime $p$ of $\ell$ bits and a Weil $p^2$-number $\pi$ corresponding to the Jacobian $J_C$ of a curve of genus 2 over $\mathbf{F}_{p^2}$ such that $\#J_C(\mathbf{F}_{p^2})$ is prime.

---

(1) Take a random positive integer $p$ of $\ell$ bits.

(2) If $p$ is prime, continue. Otherwise, go to Step 1.

(3) If $p\mathcal{O}_K$ factors as $\mathfrak{p}_1\overline{\mathfrak{p}_1}\mathfrak{p}_2$, continue. Otherwise, go to Step 1.

(4) If $\mathfrak{p}_1^2\mathfrak{p}_2$ is principal, let $\pi_0$ be a generator and let $v = \pi_0\overline{\pi_0}p^{-2} \in \mathcal{O}_{K_0}^*$. Otherwise, go to Step 1.

(5) If we have $v = N_{K/K_0}(w)$ for some $w \in \mathcal{O}_K^*$, then put $\pi = w^{-1}\pi_0$. Otherwise, go to Step 1.

(6) If $N(u\pi - 1)$ is prime for some $u \in \{\pm 1\}$, then replace $\pi$ by $u\pi$. Otherwise, go to Step 1.

(7) **return** $p, \pi$.

---

Note that the group order $N(\pi - 1)$ of $J_C$ has about $4\ell$ bits since we have $N(\pi - 1) \approx N(\pi) = p^4$.

**Theorem 9.** *If Algorithm 1 terminates, then the output is correct.*

*Fix the input field $K$ and assume that it satisfies the conditions of Lemma 7. If $K$ has no prime ideal of norm 2, and no prime above 2 is ramified in $K/K_0$, then the heuristic expected runtime of the algorithm is polynomial in $\ell$.*

*Proof.* The output $\pi$ is a Weil $p^2$-number satisfying the conditions of Lemma 1, and the corresponding abelian surface $A$ has $\#A(\mathbf{F}_{p^2}) = N(\pi - 1)$ rational points, which proves that the output is correct.

All numbers we encounter have logarithmic absolute values and heights that are bounded linearly in $\ell$, while the field $K$ is fixed. This

shows that, using the algorithms of [16], all steps, including the primality and principality tests, as well as finding a generator of $\mathfrak{p}_1^2\mathfrak{p}_2$ and trying to extract a square root of $v$, take time polynomial in $\ell$. It therefore suffices to prove that the heuristic expected number of iterations of Step 1 is quadratic in $\ell$.

The number $p$ has a heuristic probability $1/(\ell \log 2)$ to be prime by the Prime Number Theorem. This shows that for each time Step 3 is reached, one expects to run Step 1 about $\ell \log 2$ times.

We will 'prove' that the heuristic bound holds even if we restrict in Step 3 to $\mathfrak{p}_1$ principal and generated by $\alpha$. By Lemma 7, the density of the set of primes $p$ that factor in the appropriate way and for which $\alpha$ exists is $(4h_K)^{-1}$, so we arrive at Step 4 (with $\mathfrak{p}_1 = (\alpha)$) with probability $(4h_K)^{-1}$.

Note that $\pi = -\alpha\overline{\alpha}^{-1}p$ is a generator of $\mathfrak{p}_1^2\mathfrak{p}_2$, so we pass Step 4 with $\pi_0 = w\pi$ for some unit $w \in \mathcal{O}_K^*$.

Note that we have $p^2 = \pi\overline{\pi}$, hence $v = w\overline{w}$, proving that we pass Step 5 as well.

We now only need to show that $N(\pi - 1)$ is prime with sufficiently high probability. Treating $\alpha$ as a random element of $\mathcal{O} = \mathcal{O}_K$, we wish to know the probability that $X = N(\pi - 1)$ is prime, i.e., not divisible by any prime $q < X$. For each such $q$, we consider the homomorphism

$$\varphi : (\mathcal{O}/q\mathcal{O})^* \to (\mathcal{O}/q\mathcal{O})^* : x \mapsto x\overline{x}^{-1}N(x),$$

which sends $(\alpha \bmod q)$ to $(-\pi \bmod q)$. Now we have $q | N(\pi - 1)$ if and only if $\pi \equiv 1 \pmod{\mathfrak{q}}$ for some prime $\mathfrak{q} | q$ of $K$. Let $\varphi_{\mathfrak{q}}$ be the composition of $\varphi$ with the natural map $(\mathcal{O}/q\mathcal{O})^* \to (\mathcal{O}/\mathfrak{q})^*$. Note that we have $\pi \equiv 1 \pmod{\mathfrak{q}}$ if and only if $\alpha$ is an element of $\varphi_{\mathfrak{q}}^{-1}(-1)$. If we define

$$P_q = 1 - \frac{\#\bigcup_{\mathfrak{q}|q} \varphi_{\mathfrak{q}}^{-1}(-1)}{\#(\mathcal{O}/q\mathcal{O})^*},$$

then the heuristic probability of $q \nmid N(\pi - 1)$ equals $P_q$. As the homomorphism $\varphi$ sends 1 to 1, we find $P_q > 0$ for all $q > 2$.

For $q = 2$, note that we have $N(x) = 1$. Then for all $\mathfrak{q} \mid q$ with $\overline{\mathfrak{q}} = \mathfrak{q}$, take $(x \bmod \mathfrak{q}) \in (\mathcal{O}/\mathfrak{q})^*$ with $x \neq \overline{x}$, which is possible, because 2 is unramified in $K/K_0$. For $\mathfrak{q} \mid q$ with $\overline{\mathfrak{q}} \neq \mathfrak{q}$, take exactly one of $(x \bmod \mathfrak{q})$ and $(x \bmod \overline{\mathfrak{q}})$ equal to 1, which is possible because $\mathfrak{q}$ has norm $\geq 4$. Then $x\overline{x}^{-1} \not\equiv 1 \equiv -1 \pmod{\mathfrak{q}}$ for all $\mathfrak{q} \mid q$, which proves $P_2 > 0$.

We use the lower bound $P_q > 0$ for $q \leq 17$.

For $q \geq 19$, note that we have

$$P_q \geq 1 - \sum_{\mathfrak{q}|q} \frac{\#\ker \varphi_{\mathfrak{q}}}{\#(\mathcal{O}/q\mathcal{O})^*} \geq 1 - \sum_{\mathfrak{q}|q} \frac{1}{\#\operatorname{im} \varphi_{\mathfrak{q}}}$$

and that $\operatorname{im} \varphi_{\mathfrak{q}} \supset \varphi_{\mathfrak{q}}(\mathbf{F}_q^*) = (\mathbf{F}_q^*)^4$ has order $\geq (q-1)/4$, hence we have

$$P_q \geq 1 - 4\frac{4}{q-1} > 1 - \frac{17}{q}.$$

We thus find heuristically that $N(\pi - 1)$ is prime with probability at least a positive constant times

$$Y = \prod_{\substack{19 \leq q < X \\ \text{prime}}} \left(1 - \frac{17}{q}\right).$$

We find $\log(Y) > -\sum_q \frac{17}{q}$, and the right hand side, by Mertens' theorem [39, Thm. 427 in 22.7], is $17 \log\log X$ plus something that converges to a constant if $X$ tends to infinity. In particular, we find that $1/Y$ is at most polynomial in $\log X \approx 4\ell$, which is what we needed to prove. □

**Remark 10.** For more detailed heuristics on prime order Jacobians of curves of genus 2 than what is in the proof of Theorem 9, see Weng [96, §5.2.2].

**Remark 11.** The conditions of Lemma 7 are sufficient in Theorem 9 and, as we said before, they hold for 'most' non-Galois quartic CM-fields. They are however not necessary, and we give strictly weaker conditions in Section 6.

The following lemma shows that the conditions on the decomposition of 2 in $K$ are necessary in Theorem 9, and that these conditions are not specific to $p$-rank 1, or even to abelian surfaces. These conditions vanish however if one allows the group order to be 'almost prime' in the sense that it is a prime times a 'small' (say $\leq 16$) positive integer.

**Lemma 12.** *Let $\pi$ be the Frobenius endomorphism of an abelian variety $A$ over a finite field $k$ of odd characteristic, and let $K = \mathbf{Q}(\pi)$. If one of the following conditions holds, then the order of $A(k)$ is even.*

*(1) $K$ has a prime ideal $\mathfrak{q}$ of norm 2,*

*(2) $K$ is totally real, or*

*(3) $K$ is a CM-field with totally real subfield $K_0$ and $K$ has a prime ideal $\mathfrak{q}|2$ that is ramified in $K/K_0$.*

*Proof.* If $\mathfrak{q}$ has norm 2, then we have $\pi \not\equiv 0 \pmod{\mathfrak{q}}$, hence $\pi - 1 \equiv 0 \pmod{\mathfrak{q}}$, which implies $2|N(\pi - 1)$.

In the other two cases, complex conjugation is trivial on the group $(\mathcal{O}/\mathfrak{q})^*$ of odd order. Note that $\pi\overline{\pi} \in \mathbf{Q}$ implies that $\pi^2 = \pi\overline{\pi}$ is trivial in that group, hence so is $\pi$. We see again that $\pi - 1 \equiv 0 \pmod{\mathfrak{q}}$ implies $2|N(\pi - 1)$. □

Our second algorithm is a modification of Algorithm 1 in which we start with an element $\alpha \in \mathcal{O}_K$, instead of with a prime $p$, and check if $p = N(\alpha)$ is a prime that decomposes in the appropriate manner. We use Algorithm 2 as a stepping stone towards Algorithm 3, which allows one to prescribe the embedding degree of the output by imposing congruence conditions on $\alpha$.

---

**Algorithm 2.**
**Input:** A non-Galois CM-field $K$ of degree 4 and a positive integer $\ell$.
**Output:** A prime $p$ of $\ell$ bits and a Weil $p^2$-number corresponding to the Jacobian $J_C$ of a curve $C$ of genus 2 over $\mathbf{F}_{p^2}$ such that $J_C$ has $p$-rank 1 and a prime number of $\mathbf{F}_{p^2}$-rational points.

---

(1) Take a random element $\alpha$ of $\mathcal{O}_K$ of which the norm $N(\alpha)$ has $\ell$ bits.

(2) If $p = N(\alpha)$ is prime in $\mathbf{Z}$, continue. Otherwise, go to Step 1.

(3) If the prime $\beta = p\alpha^{-1}\overline{\alpha}^{-1}$ of $\mathcal{O}_{K_0}$ remains prime in $\mathcal{O}_K$, then let $\pi = \alpha^2\beta$. Otherwise, go to Step 1.

(4) If $N(u\pi - 1)$ is prime for some $u \in \{\pm 1\}$, then replace $\pi$ by $u\pi$. Otherwise, go to Step 1.

(5) **return** $p, \pi$.

---

**Theorem 13.** *If Algorithm 2 terminates, then the output is correct.*

*Fix the input field $K$ and assume that it satisfies the conditions of Lemma 7. If $K$ has no prime ideal of norm 2, and no prime above 2 is ramified in $K/K_0$, then the heuristic expected runtime of the algorithm is polynomial in $\ell$.*

*Proof.* By Lemma 6, the output $\pi$ is a Weil $p^2$-number satisfying the conditions of Lemma 1, and the corresponding abelian surface $A$ has $\#A(\mathbf{F}_{p^2}) = N(\pi - 1)$ rational points, which proves that the output is correct.

Lemma 7 shows that among the elements $\alpha$ of $\mathcal{O}_K$ of prime norm, at least about 1 in every $4h_K$ has the appropriate factorization, so if we treat $N(\alpha)$ and $N(\pi-1)$ as random integers as we did in the proof of Theorem 9, then we find again that the heuristic expected runtime is polynomial in $\ell$. □

**Remark 14.** Actually, the heuristic probability of passing from Step 3 to Step 4 in Algorithm 2 is 1/2 instead of only $(4h_K)^{-1}$ as can be seen by applying Chebotarev's density theorem to the quadratic extension $LH/H$ from the proof of Lemma 7.

Algorithm 3 constructs $p$-rank-1 curves with prescribed embedding degree by imposing congruence conditions on $\alpha$ in a way that is similar to what is done in the algorithm of Freeman, Stevenhagen, and Streng [26].

---

**Algorithm 3.**
**Input:** A non-Galois CM-field $K$ of degree 4, a positive integer $\kappa$ and a prime number $r \equiv 1 \pmod{2\kappa}$ that splits completely in $K$.
**Output:** A prime $p$ and a Weil $p^2$-number $\pi$ corresponding to the Jacobian $J_C$ of a curve $C$ of genus 2 over $\mathbf{F}_{p^2}$ that has $p$-rank 1 and embedding degree $\kappa$ with respect to a subgroup of order $r$.

---

(1) Let $\mathfrak{r}$ be a prime of $K$ dividing $r$, let $\mathfrak{s} = r\mathfrak{r}^{-1}\overline{\mathfrak{r}}^{-1}$ and compute a basis $b$ of $\mathcal{O}_K$.

(2) Take a random element $x$ of $\mathbf{F}_r^*$ and a primitive $2\kappa$-th root of unity $\zeta \in \mathbf{F}_r^*$.

(3) Take the 'small' $\alpha \in \mathcal{O}_K$ such that $\alpha \bmod \mathfrak{r} = x$, $\alpha \bmod \overline{\mathfrak{r}} = x\zeta$ and $\alpha \bmod \mathfrak{s} = x^{-1}$. Here 'small' means that the coordinates with respect to the basis $b$ are $\leq r/2$.

(4) If $p = N_{K/\mathbf{Q}}(\alpha)$ is prime in $\mathbf{Z}$, continue. Otherwise, go to Step 2.

(5) If the prime $\beta = p\alpha^{-1}\overline{\alpha}^{-1}$ of $\mathcal{O}_{K_0}$ remains prime in $\mathcal{O}_K$, let $\pi = \alpha^2\beta$. Otherwise, go to Step 2.

(6) **return** $p, \pi$.

---

**Theorem 15.** *If Algorithm 3 terminates, then the output is correct. If the input field $K$ is fixed and satisfies the conditions of Lemma 7, then the heuristic expected runtime of the algorithm is polynomial in $r$.*

*Proof.* The facts that the output has $p$-rank 1 and a Jacobian of order $N(\pi - 1)$ are proven as in the proof of Theorem 13.

If $r$ divides the group order $N(\pi - 1)$, then the embedding degree is the order of $(p^2 \bmod r)$ in the group $\mathbf{F}_r^*$ (see also [26, Proposition 2.1]). So to prove that $J_C$ has embedding degree $\kappa$ with respect to $r$, it suffices to prove that $p^2 \bmod r$ is a primitive $\kappa$-th root of unity in $\mathbf{F}_r^*$ and that $r$ divides $N(\pi - 1)$.

Let $\phi$ be the non-trivial automorphism of $K_0$. Then we have $\beta = \phi(\alpha\overline{\alpha})$, hence $\pi \bmod \mathfrak{r} = (\alpha \bmod \mathfrak{r})^2(\phi(\alpha\overline{\alpha}) \bmod \mathfrak{r})$. Inside $\mathbf{F}_r$, we have

$$\begin{aligned}(\phi(\alpha\overline{\alpha}) \bmod \mathfrak{r}) &= (\alpha\overline{\alpha} \bmod \mathfrak{s}) = (\alpha \bmod \mathfrak{s})(\alpha \bmod \overline{\mathfrak{s}}) \\ &= (\alpha \bmod \mathfrak{s})^2 = x^{-2},\end{aligned}$$

hence we have $(\pi \bmod \mathfrak{r}) = 1$, so $r$ divides $N(\pi - 1)$. Moreover,

$$\begin{aligned}(p^2 \bmod r) &= (p^2 \bmod \mathfrak{r}) = (\alpha \bmod \mathfrak{r})^2(\overline{\alpha} \bmod \mathfrak{r})^2(\phi(\alpha\overline{\alpha}) \bmod \mathfrak{r})^2 \\ &= (\alpha \bmod \mathfrak{r})^2(\alpha \bmod \overline{\mathfrak{r}})^2 x^{-4} = \zeta^2\end{aligned}$$

is a primitive $\kappa$-th root of unity.

This finishes the proof of the correctness of the output. Next we prove the heuristic runtime. As $r$ splits completely, $\alpha$ is a lift of some element modulo $r$. We treat its norm $p = N(\alpha)$ as a random integer of $4\log_2 r$ bits. The rest of the proof is as the proof of Theorem 13. □

**Remark 16.** Actually, the prime $r$ does not need to split completely in Algorithm 3. It suffices to have $r\mathcal{O}_K = \mathfrak{r}\overline{\mathfrak{r}}\mathfrak{s}$, where $\mathfrak{r}$ is prime and $\mathfrak{s}$ may be prime or composite.

**Remark 17.** Note that if Algorithm 2 or 3 terminates, then $K$ satisfies the conditions of Lemma 7, which are therefore not only sufficient, but also necessary for each of these algorithms to terminate.

Let $A$ be a $g$-dimensional abelian variety over the finite field $k$ of $q$ elements. Its *$\rho$-value* with respect to a subgroup of $A(k)$ of order $r$ is defined to be $\rho = g\log q/\log r$. As we have $\log \#A(k) \approx g\log q$, the $\rho$-value measures the ratio between the bit size of $r$ and the bit size of the order of the full group of rational points on $A$. It is at least about 1 if $q$ is large. If we have $A = J_C$, then a point on $A$ can be represented by a $g$-tuple of points on $C$, hence $\rho$ is also the ratio between the bit size of a group element of $A$ and the bit size of $r$. For cryptography, one wants the $\rho$-value to be as small as possible to save bandwidth when transmitting points on $J_C$.

The prime $p$, computed as the norm of the element $\alpha$ in Step 4, is expected to satisfy $\log(p) \approx 4\log(r)$. Since our $p$-rank-1 curve is defined over $\mathbf{F}_{p^2}$, its $\rho$-value is $\rho = 2\log(p^2)/\log(r) \approx 16$. For a more

detailed version of this heuristic analysis of the $\rho$-value, see Freeman, Stevenhagen, and Streng [26], who compute a $\rho$-value of about 8 for their ordinary abelian surfaces with prescribed embedding degree. For cryptographic applications, a $\rho$-value of 16 or even 8 is larger than desired, but it does show that pairing-based cryptography is possible for curves of genus 2 with $p$-rank 1.

When working with odd embedding degree $\kappa$, the *embedding field* $\mathbf{F}_p(\zeta_r)$ could be smaller than the field $\mathbf{F}_{p^2}(\zeta_r) = \mathbf{F}_{p^{2\kappa}}$ that is suggested by the embedding degree $\kappa$ (see also Hitt [42]). This may influence the security of pairing-based cryptography, but can easily be avoided by restricting to even embedding degree $\kappa$, or by only accepting primes $p$ such that $r$ does not divide $p^\kappa - 1$.

# 5 Constructing curves with given Weil numbers

We will now explain the explicit CM construction of a curve $C/\mathbf{F}_{p^2}$ such that $J(\widetilde{C})$ corresponds to our Weil $p^2$-number $\pi$. A more detailed exposition can be found in [27].

Honda's CM construction of the abelian variety corresponding to a given Weil $q$-number $\pi$ is based on the theory of *complex multiplication* of abelian varieties of Shimura and Taniyama [78, in particular §13, Thm. 1]. The analogous theory for elliptic curves is even more classical and dates back to the early 19th century. The first algorithmic application of the CM construction of elliptic curves is its application to primality proving by Atkin and Morain [1].

The construction starts by taking an abelian variety $A$ over a number field $F$ such that we have $\mathrm{End}(A) \cong \mathcal{O}_K$, where $K$ is a field containing $\pi$, and reduces this variety modulo an appropriate prime $\mathfrak{P}$ of $F$. For our $p$-rank-1 Weil numbers $\pi$, one can take $K = \mathbf{Q}(\pi)$ and any prime $\mathfrak{P}$ dividing $p$.

In the dimension-2 case, instead of writing down the abelian surface $A$ itself, one only writes down the *absolute Igusa invariants* $j_1, j_2, j_3 \in F$ of the curve $C$ of which $A$ is the Jacobian. These invariants are the first three of a set of 10 invariants given on page 641 of [45]. One then reduces the invariants modulo $\mathfrak{P}$ and, assuming $(j_1 \bmod \mathfrak{P})$ is a unit, constructs $\widetilde{C} = (C \bmod \mathfrak{P})$ from the reduced invariants using Mestre's algorithm [61]. Honda's construction shows that $J(\widetilde{C})$ or its quadratic twist corresponds to our Weil $p^2$-number $\pi$.

In all practical implementations, the invariants $j_n \in F$ are repre-

sented by polynomials $H_1, H_2, H_3$ or $H_1, \widehat{H}_2, \widehat{H}_3$ called *Igusa class polynomials*. We explain the polynomials $\widehat{H}_n$ later, but the polynomials $H_n$ are given by

$$H_n = \prod_C (X - j_n(C)),$$

where the product ranges over isomorphism classes of curves $C$ such that we have $\mathrm{End}(J(C)) \cong \mathcal{O}_K$. For every triple $(j_1, j_2, j_3)$ of zeroes $j_n \in \overline{\mathbf{F}_p}$ of $H_n$ with $j_1 \neq 0$, one thus obtains a unique $\overline{\mathbf{F}_p}$-isomorphism class of curves. Assuming $j_1(C) \notin \mathfrak{P}$ for some $C$, a twist of at least one of the curves we obtain has Weil number $\pi$. Let $\widetilde{C}$ be such a curve. As we know the group order $N(\pi - 1)$ of $J(\widetilde{C})(\mathbf{F}_{p^2})$, we can quickly check whether we have the correct curve by taking random points on its Jacobian and multiplying them by $N(\pi - 1)$.

As the field $K$ is fixed, so are its class polynomials. They can therefore be precomputed using any of the three known algorithms: the complex analytic method of Spallek [79] and van Wamelen [88], for which Streng [82] recently gave the first runtime analysis and proof of correctness, the 2-adic method of Gaudry, Houtmann, Kohel, Ritzenthaler, and Weng [32], and the Chinese remainder method of Eisenträger and Lauter [21]. Alternatively, class polynomials can be found in the ECHIDNA database [50].

The alternative class polynomials $\widehat{H}_n$ are given by

$$\widehat{H}_n = \sum_C j_n(C) \prod_{C' \not\cong C} (X - j_1(C')), \quad (n = 2, 3)$$

where both the product and the sum range over isomorphism classes of curves $C$ for which $\mathrm{End}(J(C)) \cong \mathcal{O}_K$ holds. For any such $C$, we have $j_n(C)H_1'(j_1(C)) = \widehat{H}_n(j_1(C))$. This implies that if every coefficient of $H_1$ has a denominator that is not divisible by $p$, and $(H_1 \bmod p)$ has a non-zero root of multiplicity 1, then we can compute the Igusa invariants of a curve $\widetilde{C}$, which is automatically either the curve we want or a quadratic twist. The idea of using $\widehat{H}_n$ and not the more standard Lagrange interpolation is due to Gaudry, Houtmann, Kohel, Ritzenthaler, and Weng, who show in [32] that $\widehat{H}_n$ heuristically has a much smaller height.

# 6 A sufficient and necessary condition

As said before, the condition of Lemma 7 are sufficient for all three algorithms to work and necessary for Algorithms 2 and 3. They are

also easy to check and true for 'most' non-Galois quartic CM-fields. The current section gives a weaker condition that is both sufficient and necessary for Algorithm 1 to work. We also give examples to show that this condition is non-trivial and strictly weaker than that of Lemma 7.

Let $K$ be a non-Galois CM-field of degree 4. Let $C/\overline{K}$ be a curve of genus 2 over the algebraic closure $\overline{K}$ of $K$ such that $\mathrm{End}(J_C) \cong \mathcal{O}_K$ holds. Such $C$ are known to exist. The field $\mathbf{Q}(j) \subset \overline{K}$ generated over $\mathbf{Q}$ by all 10 absolute Igusa invariants $j_1(C), \ldots, j_{10}(C)$ of [45, page 641] is called the *field of moduli* of $C$. For any subfield $X \subset \overline{K}$, let $X(j)$ be the compositum $X \cdot \mathbf{Q}(j)$. Write $K = K_0(\sqrt{r})$ for some $r \in K_0$ and let $K_0^{\mathrm{r}} = \mathbf{Q}(\sqrt{N_{K_0/\mathbf{Q}}(r)})$ (as before).

**Lemma 18.** *Let $K, K_0^{\mathrm{r}}, K(j)$ be as above and let $G$ be the Galois group of the normal closure of $K(j)$ over $\mathbf{Q}$. Let $S$ be the set of primes $p$ that factor in $K$ as $p\mathcal{O}_K = \mathfrak{p}_1\overline{\mathfrak{p}_1}\mathfrak{p}_2$ and such that there exists a Weil $p^2$-number $\pi$ such that we have $\pi\mathcal{O}_K = \mathfrak{p}_1^2\mathfrak{p}_2$.*

*The Dirichlet density of $S$ is*

$$\frac{\#\{\sigma \in G \mid \operatorname{ord}\sigma = 2, \sigma_{|K_0^{\mathrm{r}}} \neq \mathrm{id}_{K_0^{\mathrm{r}}}\}}{\#G}.$$

*If $S$ is non-empty, then it has positive density.*

**Corollary 19.** If Algorithm 1 terminates on input $K$, then $\sigma$ as in Lemma 18 exists for $K$. Conversely, if $K$ is fixed and $\sigma$ exists for $K$, then Algorithm 1 heuristically has a polynomial runtime.

*Proof of Corollary 19.* If Algorithm 1 terminates, then $S$ is non-empty, hence $\sigma$ exists by Lemma 18. If $\sigma$ exists, then the proof of Theorem 9 is valid, so Algorithm 1 heuristically has a polynomial runtime. □

To prove Lemma 18, we need some more theory. Let $L$ be the normal closure of $K$. A *CM-type* of $K$ is a set $\Phi$ of two embeddings $\varphi : K \to L$ that satisfies $\Phi \cap \overline{\Phi} = \emptyset$. Let $C$ be a curve as above, and let $\Phi = \{\varphi_1, \varphi_2\}$ be its CM-type as defined in [78, §5.2]. The exact definition of this CM-type will not be important to us.

The *reflex field*

$$K^{\mathrm{r}} = \mathbf{Q}(\textstyle\sum_i \varphi_i(x) : x \in K) \subset L$$

of $K$ with respect to $\Phi$ is one of the two non-Galois CM subfields of $L$ of degree 4 that are not conjugates of $K$. Its real quadratic subfield $K_0^{\mathrm{r}}$ does not depend on $\Phi$ and is exactly the field $K_0^{\mathrm{r}}$ that we have seen above Lemma 7. By [77, Prop. 20.3(i)], we have $K_0^{\mathrm{r}} \subset \mathbf{Q}(j)$, so that we have the inclusions of fields shown in Figure V.1.

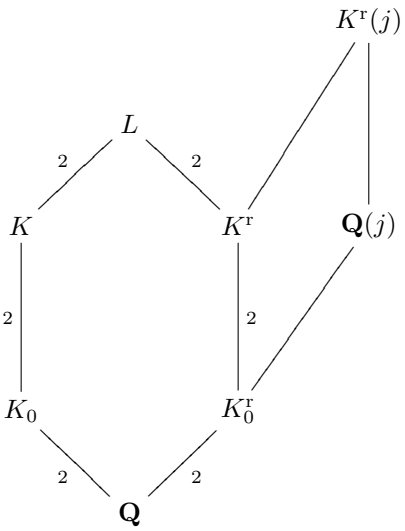



Figure V.1: Inclusions between the fields

The main theorem of complex multiplication gives $K^{\mathrm{r}}(j)$ as an unramified abelian extension of $K^{\mathrm{r}}$. To state it, we need to define the *type norm* of the *reflex type* of $\Phi$. Let $\Phi_L$ be the set of extensions of elements of $\Phi$ to $L$, so $\Phi_L$ is a CM-type of $L$ and so is the set $\Phi_L^{-1}$ of inverses of elements of $L$. The set of restrictions of $\Phi_L^{-1}$ to $K^{\mathrm{r}}$ is a CM-type $\Phi^{\mathrm{r}} = \{\psi_1, \psi_2\}$ of $K^{\mathrm{r}}$ called the *reflex* of $\Phi$ [78, §8.3]. By [78, §8.3 Prop. 29], for any fractional $\mathcal{O}_{K^{\mathrm{r}}}$-ideal $\mathfrak{a}$, there is a unique fractional $\mathcal{O}_K$-ideal $N_{\Phi^{\mathrm{r}}}(\mathfrak{a})$ such that we have

$$N_{\Phi^{\mathrm{r}}}(\mathfrak{a})\mathcal{O}_L = \prod_{i=1}^{2} \psi_i(\mathfrak{a})\mathcal{O}_L.$$

The map $N_{\Phi^{\mathrm{r}}}$ from ideals of $K^{\mathrm{r}}$ to ideals of $K$ is called the *type norm* with respect to $\Phi^{\mathrm{r}}$.

**Theorem 20** (Main Theorem 1 in §15.3 of [78])**.** *The field extension $K^{\mathrm{r}}(j)/K^{\mathrm{r}}$ is abelian and unramified. Its Galois group corresponds via the Artin map to $\mathrm{Cl}_{K^{\mathrm{r}}}/H_0$, where $H_0$ is the group of ideal classes $[\mathfrak{a}]$ such that $N_{\Phi^{\mathrm{r}}}(\mathfrak{a})$ is principal and generated by an element $\mu \in K$ with $\mu\overline{\mu} \in \mathbf{Q}^*$.* □

The following lemma computes $N_{\Phi^{\mathrm{r}}}(\mathfrak{q})$ for certain primes $\mathfrak{q}$.

**Lemma 21.** *Let $K$ be a quartic CM-field and $p$ a prime that factors in $K$ as $p\mathcal{O}_K = \mathfrak{p}_1\overline{\mathfrak{p}_1}\mathfrak{p}_2^e$.*

*(1) The prime $p$ factors in $K_0^{\mathrm{r}}$ as $\mathfrak{s}^e$ for a prime $\mathfrak{s}$, which splits in $K^{\mathrm{r}}$ as $\mathfrak{s}\mathcal{O}_{K^{\mathrm{r}}} = \mathfrak{q}\overline{\mathfrak{q}}$; and*

*(2) we have $N_{\Phi^{\mathrm{r}}}(\mathfrak{q}) = \mathfrak{p}_1^{2/e}\mathfrak{p}_2$ (up to complex conjugation).*

*Proof.* Let $\mathfrak{P} \subset \mathcal{O}_L$ be the unique prime over $\mathfrak{p}_1$. Part (1) follows from the fact that the decomposition group of $\mathfrak{P}$ is $\mathrm{Gal}(L/K)$ and that the inertia group has order $e$.

For part (2), let $s$ be the generator of $\mathrm{Gal}(L/K)$, let $s'$ be the generator of $\mathrm{Gal}(L/K^{\mathrm{r}})$ and set $r = ss'$. Then $\Phi_L \subset \mathrm{Gal}(L/\mathbf{Q})$ has 4 elements and satisfies $\Phi_L\langle s\rangle = \Phi_L$ and $\Phi_L^{-1}\langle s'\rangle = \Phi_L^{-1}$, hence $\Phi_L^{-1}$ is $\{1, s, s', ss'\}$ or its complex conjugate, and we have $\Phi^{\mathrm{r}} = \{1, s_{|K^{\mathrm{r}}}\}$ up to complex conjugation. Take $\psi_1 = 1, \psi_2 = s$. We compute

$$\begin{aligned} N_{\Phi^{\mathrm{r}}}(\mathfrak{q})\mathcal{O}_L &= (\mathfrak{q}\mathcal{O}_L)({}^s\mathfrak{q}\mathcal{O}_L) = \left(\mathfrak{P}({}^{s'}\mathfrak{P})\right)\left(({}^s\mathfrak{P})({}^{ss'}\mathfrak{P})\right) \\ &= \mathfrak{P}^2\left(({}^{s'}\mathfrak{P})({}^{ss'}\mathfrak{P})\right) = (\mathfrak{p}_1^{2/e}\mathcal{O}_L)(\mathfrak{p}_2\mathcal{O}_L), \end{aligned}$$

up to complex conjugation, which proves (2). □

*Proof of Lemma 18.* Let $p$ be a prime number that is unramified in $K$. We prove that $p$ is in $S$ if and only if its decomposition group in the normal closure of $K(j)$ is of order 2 and acts non-trivially on $K_0^{\mathrm{r}}$. Chebotarev's density theorem [66, Theorem 13.4] then proves the formula for the density. Moreover, if $S$ is non-empty, then $\sigma$ exists, hence the density is positive.

Let $p$ be a prime number and let $\sigma \in G$ be its $p$-th power Frobenius. Suppose $p$ is in $S$ and write $p\mathcal{O}_K = \mathfrak{p}_1\overline{\mathfrak{p}_1}\mathfrak{p}_2$. The image of $\sigma$ in $\mathrm{Gal}(L/\mathbf{Q})$ generates $\mathrm{Gal}(L/K)$ or its conjugate, hence has order 2. It follows that $p$ is inert in $K_0^{\mathrm{r}}/\mathbf{Q}$ and splits into two factors $\mathfrak{q}$ and $\overline{\mathfrak{q}}$ in $K^{\mathrm{r}}$. Lemma 21 shows that the type norm of $\mathfrak{q}$ is $N_{\Phi^{\mathrm{r}}}(\mathfrak{q}) = \mathfrak{p}_1^2\mathfrak{p}_2 = \pi\mathcal{O}_K$ or its complex conjugate, and we have $\pi\overline{\pi} \in \mathbf{Q}^*$, so we find $[\mathfrak{q}] \in H_0$, hence $\sigma^2$ is trivial on $K^{\mathrm{r}}(j)$ and in particular on $\mathbf{Q}(j)$.

Recall that $\mathbf{Q}(j)$ is the field generated over $\mathbf{Q}$ by the absolute Igusa invariants of $C$ and that $C$ is any curve with CM by $\mathcal{O}_K$. In particular, we can replace $C$ by ${}^{\tau}C$ for any automorphism $\tau$ of $\overline{K}/\mathbf{Q}$. This shows that $\sigma^2$ is also trivial on ${}^{\tau}\mathbf{Q}(j)$ for any $\tau$, and hence $\sigma^2$ is trivial on the normal closure of $\mathbf{Q}(j)$. As it is also trivial on the normal closure $L$ of $K$, we find that it is trivial on the normal closure of $K(j)$ and hence $\sigma$ is in the set of Lemma 18.

Conversely, suppose that $\sigma^2$ is trivial and $\sigma$ is non-trivial on $K_0^{\mathrm{r}}$. As $\sigma_{|L}$ generates $\mathrm{Gal}(L/K)$ or a conjugate, we find that $p$ factors as

$p\mathcal{O}_K = \mathfrak{p}_1\overline{\mathfrak{p}_1}\mathfrak{p}_2$. Again, the prime $p$ is inert in $K_0^{\mathrm{r}}/\mathbf{Q}$ and splits into two factors $\mathfrak{q}$ and $\overline{\mathfrak{q}}$ in $K^{\mathrm{r}}$ with type norms $\mathfrak{p}_1^2\mathfrak{p}_2$ and its complex conjugate. As we have $\sigma^2 = 1$, we find by Theorem 20 that $\mathfrak{p}_1^2\mathfrak{p}_2 = \pi\mathcal{O}_K$ holds for some $\pi \in \mathcal{O}_K$ that satisfies $\pi\overline{\pi} \in \mathbf{Q}^*$. Since also $\pi\overline{\pi}$ is positive and has absolute value $p^2$, it is a Weil $p^2$-number and $p$ is in $S$. □

**Example 22.** For the field $K = \mathbf{Q}[X]/(X^4 + 12X^2 + 2)$ of Example 8, we can find $\mathbf{Q}(j)$ in the ECHIDNA database [50] and compute that $\mathbf{Q}(j)$ contains the field $F = \mathbf{Q}(\sqrt{2+\sqrt{2}})$, which is cyclic Galois over $\mathbf{Q}$ and contains $K_0^{\mathrm{r}} = \mathbf{Q}(\sqrt{2})$. Any automorphism of $F$ of order 2 is trivial on $K_0^{\mathrm{r}}$, so the density of $S$ in Lemma 18 is 0 and none of our algorithms works for this field.

**Example 23.** For the field $K = \mathbf{Q}[X]/(X^4+20X^2+5)$, we have $13 \in S$, so that $S$ has positive density and Algorithm 1 works for $K$. However, the discriminant $d^{\mathrm{r}} = 5$ of $K_0^{\mathrm{r}} = \mathbf{Q}(\sqrt{5})$ is a prime discriminant and occurs in the prime discriminant factorization $d = (-4)\cdot(5)\cdot(-19)$ of $K_0$. This shows that $K$ does not satisfy the conditions of Lemma 7, which are therefore too strong for Algorithm 1.

# 7 Factorization of class polynomials mod $p$

While experimenting with the explicit CM construction for curves of $p$-rank 1, we found that in the (ramified) case $e = 2$ of Lemma 1, the polynomial $H_1 \bmod p$ has no roots of multiplicity 1 in $\overline{\mathbf{F}_p}$, which made working with $\widehat{H}_n$ impossible. The current section explains this phenomenon, and shows how to adapt $H_1, \widehat{H}_2, \widehat{H}_3$ to deal with this situation. We also explain the analogue of this for the situation $e = 1$, for which there is no problem.

Let $K$, $C$, and $j$ be as in Section 6. If $j_1(C) \neq 0$ is a simple root of $H_1$, which is 'usually' the case, then we have $\mathbf{Q}(j) = \mathbf{Q}(j_1(C))$ since we can compute $j_n(C)$ from $j_1(C)$ using the polynomials $\widehat{H}_2$ and $\widehat{H}_3$ as we have seen in Section 5. The Kummer-Dedekind theorem thus relates the factorization of $(H_1 \bmod p) \in \mathbf{F}_p[X]$ to the factorization of $p$ in (an order in) $\mathbf{Q}(j)$.

**Lemma 24.** *Let $p$ be a prime that factors in $K$ as $p\mathcal{O}_K = \mathfrak{p}_1\overline{\mathfrak{p}_1}\mathfrak{p}_2$, and let $n$ be the smallest positive integer such that $en$ is even and $(\mathfrak{p}_1\mathfrak{p}_2^{e/2})^n$ is generated by a Weil $p^n$-number $\pi$. Then any prime $\mathfrak{q}$ of $K^{\mathrm{r}}$ lying over $p$ decomposes in $K^{\mathrm{r}}(j)/K^{\mathrm{r}}$ into distinct primes of residue degree $en/2$.*

*Proof.* Recall from Theorem 20 that $K^{\mathrm{r}}(j)$ is the unramified abelian extension of $K^{\mathrm{r}}$ such that the Artin map induces an isomorphism

$$\mathrm{Cl}_K/H_0 \to \mathrm{Gal}(K^{\mathrm{r}}(j)/K^{\mathrm{r}}),$$

where $H_0 \subset \mathrm{Cl}_K$ is the subgroup of ideal classes $[\mathfrak{a}]$ such that $N_{\Phi^{\mathrm{r}}}(\mathfrak{a})$ is principal and generated by an element $\mu \in K$ with $\mu\overline{\mu} \in \mathbf{Q}^*$.

The Artin isomorphism sends $[\mathfrak{q}]$ to a generator of the decomposition group of $\mathfrak{q}$, so it suffices to prove that $[\mathfrak{q}]$ has order $en/2$ in the quotient group $\mathrm{Cl}_{K^{\mathrm{r}}}/H_0$. Lemma 21 computes that $N_{\Phi^{\mathrm{r}}}(\mathfrak{q}^m)$ is either $(\mathfrak{p}_1^{2/e}\mathfrak{p}_2)^m$ or its complex conjugate, so the smallest integer $m$ with $[\mathfrak{q}^m] \in H_0$ is exactly $m = en/2$. □

**Corollary 25.** Let $p, n$ be as in Lemma 24. Then $p$ splits into prime factors of residue degree $n$ in $\mathbf{Q}(j)/\mathbf{Q}$. Each factor occurs exactly $e$ times.

*Proof.* Each prime factor $\mathfrak{p}$ has residue degree $en/2$ in $K^{\mathrm{r}}(j)/K^{\mathrm{r}}$ by Lemma 24 and $2/e$ in $K^{\mathrm{r}}/\mathbf{Q}$ by Lemma 21, hence $n$ in $K^{\mathrm{r}}(j)/\mathbf{Q}$. As all ramification of $\mathfrak{p}$ takes place in $K_0^{\mathrm{r}}/\mathbf{Q}$, we find that the ramification index of $\mathfrak{p}$ in $K^{\mathrm{r}}(j)/\mathbf{Q}$ is $e$.

We have seen in Figure V.1 on page 139 that $\mathbf{Q}(j)$ contains $K_0^{\mathrm{r}}$. As the residue degree and ramification index of $\mathfrak{p}$ in $K^{\mathrm{r}}/K_0^{\mathrm{r}}$ are 1, we find that the residue degree and ramification index of $\mathfrak{p}$ are also $n$ and $e$ in $\mathbf{Q}(j)/\mathbf{Q}$. □

**Corollary 26.** If $p$ factors in $K$ as $p\mathcal{O}_K = \mathfrak{p}_1\overline{\mathfrak{p}_1}\mathfrak{p}_2^2$, then $(H_1 \bmod p) \in \mathbf{F}_p[X]$ has no roots of multiplicity 1 in $\overline{\mathbf{F}_p}$.

*Proof.* The polynomial $H_1 \in \mathbf{Q}[X]$ is monic and the denominators of the coefficients are not divisible by $p$ because they are Igusa invariants of a curve that has potential good reduction modulo $p$. Let $c \in \mathbf{Z}$ not divisible by $p$ be such that $H_1(cX)$ is in $\mathbf{Z}[X]$ and let $f \in \mathbf{Z}[X]$ be an arbitrary irreducible factor of $H_1(cX) \in \mathbf{Z}[X]$. We find an order $\mathcal{O} = \mathbf{Z}[X]/f$ in $\mathbf{Q}(j)$. Each irreducible factor $g \in \mathbf{F}_p[X]$ of $(H_1 \bmod p)$ corresponds to the prime ideal $\mathfrak{p} = (p, g(X))$ of $\mathcal{O}$. As every prime over $p$ ramifies in $\mathbf{Q}(j)/\mathbf{Q}$ by Corollary 25, we find that $\mathfrak{p}$ is either ramified or singular. By the Kummer-Dedekind theorem (Theorem 8.2 of [81]), both cases imply that the roots of $g$ have multiplicity at least 2 as roots of $H_1$. □

This shows that $H_1, \widehat{H}_1, \widehat{H}_2$ cannot be used for the case $e = 2$. To get around this, we replace $H_1$ by an irreducible factor $f \in K_0^{\mathrm{r}}[X]$ and $\widehat{H}_n$ by the unique polynomial $S_n$ of degree at most $\deg(f) - 1$

that is congruent modulo $f$ to $\widehat{H}_n(H_1/f)^{-1}$. If we write $p\mathcal{O}_{K^r} = \mathfrak{s}^2$, then $(f \bmod \mathfrak{s}), (S_2 \bmod \mathfrak{s}), (S_3 \bmod \mathfrak{s}) \in \mathbf{F}_p[X]$ can be used in exactly the same way as $(H_1 \bmod p), (\widehat{H}_2 \bmod p), (\widehat{H}_3 \bmod p)$ and do not suffer from Corollary 26.

**Corollary 27.** For all but finitely many of the primes $p$ that decompose as $p\mathcal{O}_K = \mathfrak{p}_1\overline{\mathfrak{p}_1}\mathfrak{p}_2^e$, the reduction $(H_1 \bmod p) \in \mathbf{F}_p[X]$ is a product of distinct irreducible polynomials in $\mathbf{F}_p[X]$ of degree $n$ for $n$ given in Lemma 24 (and depending on $p$).

*Proof.* We exclude the primes dividing the denominator of any coefficient of $H_1$, as well as those dividing the discriminant. Then all roots of $(H_1 \bmod p)$ in $\overline{\mathbf{F}_p}$ are simple roots. Let $f, \mathcal{O}$ be as in the proof of Corollary 26. Then $p$ does not divide the index of $\mathcal{O}$ in its maximal order. The fact that every prime of $\mathbf{Q}(j)$ has residue degree $n$ implies that every irreducible factor of $f \bmod p$ has degree $n$. □

# 8 Examples

## Algorithm 1

We provide examples of $p$-rank-1 curves $C/\mathbf{F}_{p^2}$ such that the Jacobian $J_C$ is simple and has prime order. The CM-field for all examples is $K = \mathbf{Q}(\alpha)$, where $\alpha$ is a root of the polynomial $X^4+34X^2+217 \in \mathbf{Q}[X]$, which satisfies the conditions of Lemma 7. We give the prime $p$, the coefficients $a_1$ and $a_2$ of the minimal polynomial

$$f = X^4 - a_1X^3 + (a_2 + 2p^2)X^2 - a_1p^2X + p^4$$

of the Frobenius endomorphism and the coefficients $c_i \in \mathbf{F}_{p^2}$ of the curve equation

$$C : y^2 = c_6x^6 + c_4x^4 + c_3x^3 + c_2x^2 + c_1x + c_0.$$

The group order of the Jacobian is $\#J_C(\mathbf{F}_{p^2}) = N(\pi - 1) = f(1)$. The field $\mathbf{F}_{p^2}$ is given as $\mathbf{F}_p(\sigma)$, where $\sigma^2 = -3$. Section headings describe the number of bits of the group order $\#J_C(\mathbf{F}_{p^2})$.

Each example was generated in a few seconds on a standard PC after pre-computation of the Igusa class polynomials of $K$.

**160-bit group size**

$$\begin{aligned}
p &= 924575392409, \quad a_1 = 3396725192754\\
a_2 &= 2876182159630959921399337, \quad c_6 = \sigma\\
c_4 &= 349419850452 \cdot \sigma + 621473390194\\
c_3 &= 638315825844 \cdot \sigma + 895470286740\\
c_2 &= 247903071476 \cdot \sigma + 504258872407\\
c_1 &= 494346973570 \cdot \sigma + 326558224146\\
c_0 &= 721392332677 \cdot \sigma + 210623692149
\end{aligned}$$

**192-bit group size**

$$\begin{aligned}
p &= 236691298903769, \quad a_1 = -9692493559086\\
a_2 &= -5899217227579793179188357266 3, \quad c_6 = \sigma\\
c_4 &= 144046547562595\sigma + 31854049506043\\
c_3 &= 134634542821316\sigma + 20155601614364\\
c_2 &= 159093189820788\sigma + 52669766944798\\
c_1 &= 223684436822489\sigma + 66232364455191\\
c_0 &= 206430094481010\sigma + 170879851904277
\end{aligned}$$

**256-bit group size**

$$\begin{aligned}
p &= 15511800964685067143, \quad a_1 = 2183138494024250742\\
a_2 &= -87140339122997500378256555446470066445 7, \quad c_6 = 1\\
c_4 &= 70191988773136445 39 \cdot \sigma + 8886572032497699458\\
c_3 &= 80695668001425655 48 \cdot \sigma + 11092851174307405252\\
c_2 &= 83398732082953817 93 \cdot \sigma + 13688811293938352344\\
c_1 &= 10474983032301001361 \cdot \sigma + 14509908493781086362\\
c_0 &= 48038779053473305 04 \cdot \sigma + 12900291622358663970
\end{aligned}$$

## Algorithm 3

**192-bit group size, embedding degree** 12

Let $K$ be the field $K = \mathbf{Q}[X]/(X^4+13X^2+41)$ and let $\kappa = 12$. It took a few seconds to find the smallest prime $r > 2^{192}$ that splits completely in $K$ and $\mathbf{Q}(\zeta_{12})$, which is $r = 2^{192}+18513$. We ran Algorithm 3 with input

$K, \kappa, r$. The algorithm terminated after about 11 minutes and found a prime $p$ and a Weil $p^2$ number with $p$-rank 1 and embedding degree 12 with respect to a subgroup of order $r$. Using $p$ and precomputed Igusa class polynomials, we were able to find an equation for the corresponding hyperelliptic curve $C$ in less than a second. We only give $p$, because $\pi$ and the coefficients of $C$ would take up too much space.

$$\begin{aligned} p =& 14200385659580748274763538704897708807152013603234156901461205686404970976014364663695672498066437749119607973051961772352102985564946217214869939395896863865210769614727743634581105622738519578199736230485193265027051429370512599137 9 \end{aligned}$$

# Appendix 1. The Fourier expansions of Igusa invariants

Abstract. *We show by which integers we can divide the Igusa modular forms $I_4$, $I_6'$, $I_{10}$, and $I_2I_{10}$ so that the quotient still has integral Fourier coefficients.*

Every theta constant $\theta[c]$ has a *Fourier expansion*

$$\theta[c](Z) \;=\; \sum_{T\in \mathrm{Mat}_2(\mathbf{Q})} a_T \cdot \exp\big(2\pi i\ \mathrm{Tr}(ZT)\big).$$

In fact, the definition of $\theta[c]$ in Section II.7 already tells us that this is true with

$$a_T \;=\; \sum_{\substack{n\in\mathbf{Z}^2 \\ (n+c')(n+c')^{\mathrm{t}}=T}} (-1)^{2(n+c')^{\mathrm{t}}c''} \in \mathbf{Z},$$

where $c$ is written as $c = (c', c'')$, with column vectors $n$, $c'$, and $c''$.

The functions $h_4$, $h_6$, $h_{12}$, and $h_{10}$, defined in terms of theta constants in equation II.(7.1) are modular forms for $\mathrm{Sp}_4(\mathbf{Z})$. It is known that this implies that they have a unique Fourier expansion, that moreover $a_T \neq 0$ implies that $2T$ has integral entries and even integral diagonal entries, and that we have

$$a_T = a_{U^{\mathrm{t}}TU} \quad \text{for all } U \in \mathrm{GL}_2(\mathbf{Z}).$$

Following Lemma II.7.3, we identify the Igusa invariants $I_4$, $I_6$, $I_{10}$, and $I_2I_{10}$ with the modular forms $h_4$, $h_6$, $h_{10}$, and $h_{12}$. Section II.9 requires us to use modular forms with integral Fourier expansion, and we would like to choose these functions as small as possible. In other words, we want their Fourier coefficients to be integral with gcd equal to 1. The following result supplies such functions.

**Lemma 1.1.** *The Fourier coefficients of* $2^{-2}h_4$, $2^{-2}h_6$, $2^{-12}h_{10}$, *and* $2^{-15}h_{12}$ *are integers. Moreover, each of these four modular forms has a Fourier coefficient equal to* 1.

*Proof.* Let $I$ be the set of functions on $\mathcal{H}_g$ with integral Fourier expansion. We have $\theta[c] \in 1+2I$ for $c'' = 0$ and $\theta[c] \in 2I$ for $c'' \neq 0$. As there are 6 even theta characteristics $c$ with $c'' \neq 0$, we find

$$h_{10} = \prod_{c \text{ even}} \theta[c]^2 \in 2^{12} I.$$

Moreover, we have $\theta[c]^4 \in \mathbf{Z} + 8I$, and since $h_4$ and $h_6$ are polynomials in fourth powers of theta constants, this proves $h_4$, $h_6 \in \mathbf{Z}+8I$. Table 1 gives $a_0 = 4$ for $h_4$ and $h_6$, and shows that $h_{10}$ has a coefficient $2^{12}$. This proves the lemma for all but $2^{-15}h_{12}$.

Next, consider

$$h_{12} = \sum_{C \in S} \prod_{c \in T \setminus C} \theta[c]^4,$$

where $T$ is the set of 10 even theta characteristics and $S$ is the set of 15 Göpel quadruples. In other words, the set $T \setminus C$ ranges over those subsets of $T$ of 6 elements with sum in $\mathbf{Z}^2$. We claim that no summand has only 2 factors with $c'' \neq 0$. Indeed, the other 4 factors would be the theta constants with $c'' = 0$, and their characteristics sum up to 0 mod $\mathbf{Z}^2$, showing that the 2 remaining factors are equal. This proves the claim.

Write $h_{12} = C + D$, where $C$ (resp. $D$) is the sum of those terms with at least 4 (resp. exactly 3) factors with $c'' \neq 0$. We have $C \in 2^{16} I$.

There are exactly three non-zero elements $c'' \in \{0, \frac{1}{2}\}^2$, namely $d_1 = (0, \frac{1}{2})$, $d_2 = (\frac{1}{2}, \frac{1}{2})$, and $d_3 = (0, \frac{1}{2})$. We claim

$$D \;=\; \sum_{a \in \{0,1\}^3} \Big( \prod_{i=1}^{3} \theta[(a_i d_i, d_{4-i})]^4 \Big) \Big( \prod_{\substack{c' \not\equiv \sum_{i=1}^{3} a_i d_i \\ (\mathrm{mod}\ \mathbf{Z}^2)}} \theta[(c', 0)]^4 \Big).$$

Indeed, each term on the right is a term in $D$. Conversely, every term of $D$ has exactly one factor $\theta^4$ for each $c'' = d_{3-i}$ to make the $c''$-coordinates sum up to an element of $\mathbf{Z}^2$. The sum of their $c'$-coordinates is $\sum a_i d_i$ modulo $\mathbf{Z}^2$, hence so is the sum of the $c'$-coordinates of the theta characteristics with $c'' = 0$. This proves that this term also occurs on the right, which proves the claim.

As the $\theta$'s with $c'' \neq 0$ are in $2I$ and the $\theta^4$'s with $c'' = 0$ are in

$1 + 8I$, we can replace the latter by 1 in the product and get

$$D \equiv \prod_{i=1}^{3} \Big( \theta[(0, d_i)]^4 + \theta[(d_i, d_i)]^4 \Big) \pmod{2^{15} I}.$$

Next, we show that each factor on the right is in $2^5 I$. By the symmetry in the definition of the theta constants, one can see not only $\theta[(0, d)] \in 2I$, but also $f = \theta[(d_i, d_i)] - \theta[(0, d)] \in 4I$. It follows that $\theta[(0, d)]^4 + (\theta[(0, d)] + f)^4$ is in $2^5 I$, hence $h_{12} \in 2^{15} I$. Conversely, Table 1 shows that $2^{15}$ occurs as a coefficient. □

| $(a$ | $2b$ | $c)$ | $2^{-2}h_4$ | $2^{-2}h_6$ | $2^{-12}h_{10}$ | $2^{-15}h_{12}$ |
|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 1 | 1 | 0 | 0 |
| 0 | 0 | 1 | 240 | −504 | 0 | 0 |
| 1 | 1 | 1 | 13440 | 44352 | 1 | 1 |
| 1 | 0 | 1 | 30240 | 166320 | −2 | 10 |
| 0 | 0 | 2 | 2160 | −16632 | 0 | 0 |
| 1 | 1 | 2 | 138240 | 2128896 | −16 | −88 |
| 1 | 0 | 2 | 181440 | 3792096 | 36 | −132 |
| 2 | 2 | 2 | 604800 | 24881472 | 240 | 2784 |
| 2 | 1 | 2 | 967680 | 65995776 | −240 | −8040 |
| 2 | 0 | 2 | 1239840 | 90644400 | 32 | 17600 |
| 0 | 0 | 3 | 6720 | −122976 | 0 | 0 |
| 1 | 1 | 3 | 362880 | 15422400 | 99 | 1275 |
| 1 | 0 | 3 | 497280 | 23462208 | −272 | 736 |
| 2 | 2 | 3 | 1814400 | 234311616 | −1800 | 13080 |
| 2 | 1 | 3 | 2903040 | 453454848 | 2736 | −14136 |
| 2 | 0 | 3 | 2782080 | 530228160 | −1464 | −54120 |
| 3 | 3 | 3 | 3642240 | 883802304 | 15399 | 48303 |
| 3 | 2 | 3 | 5987520 | 1945345248 | −19008 | 38016 |
| 3 | 1 | 3 | 6531840 | 2818924416 | 27270 | −256410 |
| 3 | 0 | 3 | 8467200 | 3327730560 | −43920 | 1073520 |
| 0 | 0 | 4 | 17520 | −532728 | 0 | 0 |

Table 1: The Fourier coefficients of certain modular forms for $\mathrm{Sp}_4(\mathbf{Z})$. The entries next to $(a, 2b, c)$ are the coefficients $a_T$, where $T$ is the matrix $\left(\begin{smallmatrix} a & b \\ b & c \end{smallmatrix}\right)$.

**Remark 1.2.** We claimed in Remark II.7.2 that we have $h_4 = 2^2\psi_4$, $h_6 = 2^2\psi_6$, $h_{10} = -2^{14}\chi_{10}$, and $h_{12} = 2^{17}3\chi_{12}$, where $\psi_k$ is the Siegel

Eisenstein series of weight $k$ and $\chi_k$ is defined in terms of Eisenstein series in that remark. Table 1 allows us to give a proof of this claim.

Indeed, the graded ring of modular forms for $\mathrm{Sp}_4(\mathbf{Z})$ is equal to $\mathbf{C}[\psi_4, \psi_6, \psi_{10}, \psi_{12}]$ by [47], so we see $h_4 = c_4\psi_4$ and $h_6 = c_6\psi_6$ for certain constants $c_4$ and $c_6$, and we see that there are linear relations between $h_{10}$, $\psi_4\psi_6$, and $\chi_{10}$, and between $h_{12}$, $\psi_4^3$, $\psi_6^2$, and $\chi_{12}$. Using tables containing coefficients of $\psi_4$, $\psi_6$, $\chi_{10}$, and $\chi_{12}$, such as those of Resnikoff and Saldaña [68], we can find the appropriate linear relations.

It seems that the entry with $(a, 2b, c) = (3, 3, 3)$ for $\chi_{10}$ has a missing sign in the tables of Resnikoff and Saldaña, since it is the only one that does not agree with our table.

# Appendix 2. An alternative algorithm for enumerating CM abelian varieties

ABSTRACT. *We give an alternative for Algorithm II.3.1 for computing all triples* $(\Phi, \mathfrak{a}, \xi)$. *It uses the pairs* $(z, \mathfrak{b})$ *of Section I.5.3. We also generalize a much cited result from Spallek's thesis [79].*

## 2.1 Reduced pairs $(z, \mathfrak{b})$

Let $K$ be a CM-field of degree $2g$ with maximal totally real subfield $K_0$. Suppose we have $g = 2$ or, more generally, that the different of $K_0$ is principal.

In Section I.5.2, we saw that the principally polarized abelian varieties with CM by $\mathcal{O}_K$ correspond to equivalence classes of triples $(\Phi, \mathfrak{a}, \xi)$ consisting of a CM-type $\Phi$ of $K$, an fractional $\mathcal{O}_K$-ideal $\mathfrak{a}$, and an element $\xi \in K$ with $\mathcal{D}_{K/\mathbf{Q}}\mathfrak{a}\bar{\mathfrak{a}}\xi = \mathcal{O}_K$ and $\operatorname{Im}\phi\xi > 0$ for all $\phi \in \Phi$. Two such triples $(\Phi, \mathfrak{a}, \xi)$ and $(\Phi, \mathfrak{a}', \xi')$ with the same type $\Phi$ are called equivalent if there is an element $u \in K^*$ with $\mathfrak{a}' = u\mathfrak{a}$ and $\xi' = (u\overline{u})^{-1}\xi$.

In Section I.5.3, we saw that each triple $(\Phi, \mathfrak{a}, \xi)$ is given up to equivalence by $\mathfrak{a} = z\mathfrak{b}+\mathfrak{b}^{-1}$, $\xi = (z-\overline{z})^{-1}\delta^{-1}$, and $\Phi = \{\phi : K \to \mathbf{C} \mid \operatorname{Im}\phi\xi > 0\}$ with $z \in K$ and $\mathfrak{b}$ a fractional $\mathcal{O}_{K_0}$-ideal such that $z\mathfrak{b} + \mathfrak{b}^{-1}$ is an $\mathcal{O}_{K_0}$-submodule of $K$. We call two such pairs $(z, \mathfrak{b})$ *equivalent* if they give rise to equivalent triples $(\Phi, \mathfrak{a}, \xi)$ with the same CM-type $\Phi$.

Let $S$ be a complete set of representatives for the ideal class group of $\mathcal{O}_{K_0}$. For every $\mathfrak{b} \in S$, let $T_\mathfrak{b}$ be a half-open fundamental parallelepiped for translation by $\mathfrak{b}^{-2}$ in $K_0 \otimes \mathbf{R}$. Let $V$ be a union of $2^g$ half-open cones such that $V$ is a fundamental domain for multiplication by $(\mathcal{O}_{K_0}^*)^2$ in $K_0 \otimes \mathbf{R}$. Recall $I(z) = \prod_{\phi\in\Phi} |\operatorname{Im}\phi z|$ and let $N = N_{K_0/\mathbf{Q}}$.

**Lemma 2.3.** *Every equivalence class of pairs* $(z, \mathfrak{b})$ *contains a pair with*

1. $I(z)N(\mathfrak{b})^2$ *maximal in the equivalence class,*

*2.* $\mathfrak{b} \in S$,

*3.* $\operatorname{Im} z \in V$,

*4.* $\operatorname{Re} z \in T_{\mathfrak{b}}$.

*Proof.* For the fact that a maximum exists, see the analogous case of the Hilbert fundamental domain. That is, see Remark I.5.10 and [86, §I.2].

Next, note that for $u \in K_0^*$, we have $u^{-1}(z\mathfrak{b} + \mathfrak{b}^{-1}) = (u^{-2}z)(u\mathfrak{b}) + (u\mathfrak{b})^{-1}$, which does not change $I(x)N(\mathfrak{b})$, so $\mathfrak{b}$ can be taken in $S$. By taking $u$ to be a unit in $\mathcal{O}_{K_0}^*$, we even find $\operatorname{Im} z \in V$. Next, we can translate $z$ by any element of $\mathfrak{b}^{-2}$, which gives us $\operatorname{Re} z \in T_{\mathfrak{b}}$. □

**Remark 2.4.** The conditions in Lemma 2.3 are bounds of a fundamental domain for the action of $\mathrm{SL}_2(\mathcal{O}_{K_0})$ mentioned in Remark I.5.10. See [86, §I.3].

The pairs $(z, \mathfrak{b})$ of Lemma 2.3 satisfy $I(z)N(\mathfrak{b})^2 > C_g\Delta_0^{-1}$ for some constant $C_g$ depending only on $g$. For $g = 2$, this is Lemma II.6.5 with $C_2 = \pi^2/6$, and for other $g$, it is a straightforward generalization. Moreover, if we write $K = K_0(\sqrt{D})$ for some $D \in \mathcal{O}_{K_0}$, then we find $\sqrt{D} = az + b$ with $a \in \mathfrak{b}^2$, $b \in \mathcal{O}_{K_0}$. In other words, we have

$$z = \frac{\sqrt{D} - b}{a}.$$

We find $a \in \mathfrak{b}^2 \cap V'$ for the union of cones $V' = \sqrt{D}V^{-1} \subset K_0 \otimes \mathbf{R}$, and $N(a)^2 < I(\sqrt{D})N(\mathfrak{b})^2 C_g^{-1}\Delta_0$, so there are finitely many possibilities for $a$. We also find $b \in \mathcal{O}_{K_0} \cap aT_{\mathfrak{b}}$, which yields finitely many possibilities for $b$.

Assuming we can compute the unit group and class group of $K_0$, as well as all elements $a \in \mathfrak{b}^2$ below a given norm bound up to multiplication by $(\mathcal{O}_{K_0}^*)^2$, this gives us the following algorithm.

---

**Algorithm 2.5.**
**Input:** A CM-field $K = K_0(\sqrt{D})$ such that the different of the totally real subfield $K_0$ is principal, and a CM-type $\Phi$ of $K$. A $\mathbf{Z}$-basis of $\mathcal{O}_K$.
**Output:** At least one representative $(z, \mathfrak{b})$ of every equivalence class.

---

1. Compute a set of representatives $S$ of the class group of $K_0$.
2. Write each element of the $\mathbf{Z}$-basis of $\mathcal{O}_K$ in the form $x_i + y_i\sqrt{D}$ with $x_i, y_i \in K_0$.

3. For each $\mathfrak{b} \in S$, compute all $a \in \mathfrak{b}^2$ up to multiplication by $(\mathcal{O}_{K_0}^*)^2$ such that such that (1) $\phi(a) > 0$ holds for all $\phi \in \Phi$ and (2) we have
$$|N(a)| \leq N(\mathfrak{b})^2 \sqrt{|N(D)|} \Delta_0 C_g^{-1}.$$
4. For each pair $(\mathfrak{b}, a)$ compute a half-open fundamental domain $T_{a\mathfrak{b}^{-2}}$ for translation by $a\mathfrak{b}^{-2}$ in $\mathbf{R}^2$.
5. For each $(\mathfrak{b}, a)$, compute all $b \in \mathcal{O}_{K_0} \cap T_{a\mathfrak{b}^{-2}}$ for which $a$ divides $b^2 - D$.
6. For each triple $(\mathfrak{b}, a, b)$ and each basis element $x_i + y_i\sqrt{D}$ of $\mathcal{O}_K$, check if $y_i a \in \mathfrak{b}^2$, $x_i \pm y_i b \in \mathcal{O}_{K_0}$, and $a^{-1}y_i(D - b^2) \in \mathfrak{b}^{-2}$ hold. Remove the triple from the list if one of these conditions is not satisfied.
7. For each triple $(\mathfrak{b}, a, b)$, return the pair $(z, \mathfrak{b})$ for $z = (\sqrt{D} - b)/a$.

---

After running this algorithm, there may still be duplicate elements in the list. It is possible to eliminate them by taking only the pairs $(z, \mathfrak{b})$ that satisfy the conditions of Lemma 2.3, and by using the appropriate identifications of the boundaries of the Hilbert fundamental domain as in [86, §I.3].

Another way to remove duplicates is to use the $\mathrm{Sp}_4(\mathbf{Z})$-reduction algorithm II.5.9 followed by the algorithm of Lemma II.5.20.

## 2.2 Real quadratic fields

In the case $g = 2$, as $K_0$ is quadratic, the class group and the fundamental unit can be computed using the theory of *reduced indefinite binary quadratic forms* as was done by Shanks [74, 75]. It is relatively straightforward to derive from that theory a method for enumerating the elements of norm below a bound $B$, and we do that below. We use Lenstra [56] as our main reference.

Actually, we show how to compute the group of totally positive units $\mathcal{O}_{K_0}^{*+}$ and the strict class group $\mathrm{Cl}^+(K_0)$ of fractional ideals modulo $K_0^{*+}$, but it is easy to check if an element of $\mathcal{O}_{K_0}^*$ is a square and thus compute the class group and unit group.

We study (indefinite) binary quadratic forms $ax^2 + bxy + cy^2$ over $\mathbf{Z}$ with *discriminant* $b^2 - 4ac$ equal to $\Delta_0 > 0$. To each such form, we associate the fractional $\mathcal{O}_{K_0}$-ideal
$$\mathbf{Z} + \frac{\sqrt{\Delta_0} - b}{2a}\mathbf{Z}.$$

This gives a bijection between the set of binary quadratic forms of discriminant $\Delta_0$, and the set of fractional $\mathcal{O}_{K_0}$-ideals provided with a $\mathbf{Z}$-basis with first basis element 1. This bijection induces in turn a bijection between $\mathrm{Cl}^+(K_0)$ and the set of forms up to $\mathrm{SL}_2(\mathbf{Z})$ ([56, §3]). An indefinite quadratic form is called *reduced* if

$$\left|\sqrt{\Delta_0} - 2|a|\right| \;<\; b \;<\; \sqrt{\Delta_0}$$

holds, and called *almost-reduced* if $b$ is in the interval $J_a$, defined by

$$J_a = \begin{cases} \;]-|a|, |a|] & \text{if } |a| > \sqrt{\Delta_0}, \\ \;]\sqrt{\Delta_0} - 2|a|, \sqrt{\Delta_0}[ & \text{otherwise.} \end{cases}$$

We call an ideal *reduced* if it corresponds to a reduced form. Every class in $\mathrm{Cl}^+(K_0)$ contains a reduced ideal, and the following linear-time algorithm computes an equivalent reduced form for any input form.

---

**Algorithm 2.6.**
**Input:** a binary quadratic form $(a, b, c)$ of discriminant $\Delta_0$.
**Output:** an $\mathrm{SL}_2(\mathbf{Z})$-equivalent reduced form.

---

1. Set $(a, b, c) \leftarrow (c, -b, a)$.
2. Let $b' \in J_a$ be equivalent to $b$ modulo $2a$ and let $c' = (b^2 - \Delta_0)/(4a)$. Set $(a, b, c) \leftarrow (a, b', c')$.
3. If $(a, b, c)$ is not reduced, go to step 1.

---

For the fact that this algorithm is linear-time, see [56, Section 4]. If we apply this algorithm to a reduced form $f$, then it stops after a single iteration and returns another reduced form $\rho(f)$. The map $\rho$ is a permutation of the set of reduced forms and two reduced forms are $\mathrm{SL}_2(\mathbf{Z})$-equivalent if and only if they are in the same $\langle\rho\rangle$-orbit ([56, Section 5]).

We can now start by listing all reduced forms. We then repeatedly apply $\rho$ to partition them into $\langle\rho\rangle$-orbits. While doing this, we also compute a set of representatives $S$ of the $\langle\rho\rangle$-orbits. Every time we apply $\rho$, if we have $f_2 = \rho(f_1)$ and the ideal $\mathfrak{b}_j$ corresponds to the form $f_j$, we can compute the element $x \in K_0^*$ satisfying $\mathfrak{b}_2 = x\mathfrak{b}_1$. The unit group $\mathcal{O}_{K_0}^{*+}$ is generated by the $x$ that we get if we repeatedly apply $\rho$ to $\mathcal{O}_{K_0}$ until we get $\mathcal{O}_{K_0}$ back.

More sophisticated methods use *short representations* of $x$ and compute those not by repeatedly applying $\rho$ but by moving through the cycle of reduced ideals in a smarter way as in Buchmann, Thiel, and Williams [10]. For our running time bounds, writing out $x$ is fast enough.

Now that we have the class group and unit group, we show how to enumerate all ideals of norm at most $B$. The norm of the ideal corresponding to $(a, b, c)$ is $1/a$ by [56, Section 2]. Using only the $\mathrm{SL}_2(\mathbf{Z})$-transformations

$$T = \begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix} \quad (m \in \mathbf{Z}),$$

which changes only the second basis element, one can make a quadratic form almost-reduced (step 2 of Algorithm 2.6). In particular, every ideal $\mathfrak{b}$ with $B \cap \mathbf{Q} = \mathbf{Z}$ comes from an almost-reduced form. In particular, the ideals of norm below $B$ are exactly the ideals $n\mathfrak{b}^{-1}$ with $n \in \mathbf{Z}$ and $\mathfrak{b}$ corresponding to an almost-reduced form $(a, b, c)$ with $an^2 \leq B$. Therefore, we enumerate all almost-reduced forms with $a \leq B$. If we apply the reduction algorithm to them, then we either end up with $\mathcal{O}_{K_0}$ or with an element of $S$ that does not represent the trivial ideal class. In particular, we either know a generator or know that it is non-principal. This gives us all elements of norm at most $B$ up to the action of the unit group.

Next, we bound the running time of the algorithms we have just described. Enumerating all reduced forms takes time $\widetilde{O}(\Delta_0)$, simply by enumeration of all pairs $a$, $b$ satisfying the definition of 'reduced' and checking if $\Delta_0 - b^2$ is divisible by $4a$. If we denote the number of divisors of $n$ by $d(n)$, then it is well known that we have $d(n) = O(n^\epsilon)$ for every $\epsilon > 0$ (see e.g. [39, Thm. 315 in XVIII]). The number of reduced forms is therefore easily seen to be at most

$$\sum_{b=1}^{\lfloor\sqrt{\Delta_0}\rfloor} d(\Delta_0 - b^2) = O(\Delta_0^{\frac{1}{2}+\epsilon}).$$

If $h_0$ is the class number of $K_0$, and $R_0$ is its regulator, then the length of each $\rho$-orbit satisfies

$$\tfrac{1}{2} l \log 2 < R_0 < \tfrac{1}{2} l \log \Delta_0$$

by [56, (11.4)]. In particular, we have

$$R_0 h_0 < \tfrac{1}{2} (\log \Delta_0) \sum l = O(\Delta_0^{\frac{1}{2}+\epsilon}),$$

which one could also derive from the class number formula.

Computing the fundamental unit by walking along one $\rho$-orbit takes $l < 2R_0/\log 2 = O(\Delta_0^{1/2+\epsilon})$ steps. It involves numbers of which the height increases by something polynomial in $\log \Delta_0$ at each step, hence it takes time $O(\Delta_0^{1+\epsilon})$ using fast multiplication. We get that the whole class group and unit group algorithm we just described takes time $O(\Delta_0^{1+\epsilon})$.

Listing all almost-reduced forms with $a \leq B$ takes time $\widetilde{O}(B^2)$, where we use $\widetilde{O}(X)$ to mean "up to factors that are at most polynomial in $\log X$ and $\log \Delta_0$." Each has a bit size that is $O(\log \Delta_0)$, hence the linear-time reduction algorithm takes time $O(\log \Delta_0)$ for each of them. It needs to be run at most $2R_0/\log 2$ times and hence finds a generator that has height $\widetilde{O}(R_0)$. We find that determining all elements of norm at most $B$ (up to $(\mathcal{O}_{K_0}^*)^2$) takes time $\widetilde{O}(R_0 B^2)$.

## 2.3 Analysis of Algorithm 2.5

Let $K$ be a quartic CM-field with real quadratic subfield $K_0$ and suppose we apply Algorithm 2.5 to $K$. Step 1 computes the unit group in time $\widetilde{O}(\Delta_0)$. Step 2 is polynomial-time. In step 3, we compute the elements $a \in \mathfrak{b}^2$ by listing the integral ideals $a\mathfrak{b}^{-2}$ of norm at most $B = \sqrt{|N(D)|}\Delta_0 C_g^{-1} = \widetilde{O}(\Delta_1^{1/2}\Delta_0)$. This takes time $\widetilde{O}(R_0 B^2)$ (by the method of the previous section) for each of the $h_0$ possibilities for $\mathfrak{b}$. The total time is $O(\Delta_1 \Delta_0^{5/2+\epsilon})$.

For each of the $h_0$ ideals $\mathfrak{b}$, the number of $a$'s is at most the number of ideals of norm at most $B$, which is $\widetilde{O}(B)$ for any quadratic field.

The ideal $a\mathfrak{b}^{-2}$ was given by a 'small' basis even before we computed $a$. Therefore, we get a very reasonable fundamental parallelogram $T_{a\mathfrak{b}^{-2}}$ efficiently, and can enumerate the $b$'s in almost linear time. The number of $b$'s found in step 5 for each $(\mathfrak{b}, a)$ is at most $N(a\mathfrak{b}^{-2}) \leq B$.

There were $\widetilde{O}(h_0 B)$ pairs $(\mathfrak{b}, a)$, so the time needed for step 5 is at most $\widetilde{O}(h_0 B^2) = \widetilde{O}(\Delta_1 \Delta_0^{5/2})$. At the end of step 5, we then have at most $\widetilde{O}(h_0 B^2)$ triples $(\mathfrak{b}, a, b)$.

The ideal $a\mathfrak{b}^{-2}$ was given by a 'small' basis even before we computed $a$. Therefore, we get a very reasonable fundamental parallelogram $T_{a\mathfrak{b}^{-2}}$ efficiently, and can enumerate the $b$'s in almost linear time. The number of $b$'s found in step 5 for each $(\mathfrak{b}, a)$ is at most $N(a\mathfrak{b}^{-2}) \leq B$. There were $\widetilde{O}(Bh_0)$ pairs $(\mathfrak{b}, a)$, so this step takes time at most $\widetilde{O}(B^2 h_0) = \widetilde{O}(\Delta_1 \Delta_0^{5/2})$.

At the end of step 5, we then have at most $\widetilde{O}(h_0 B^2)$ triples $(\mathfrak{b}, a, b)$. Writing out $a$ for each triple gives an extra factor $R_0$ in the running

time, so we get a running time of $\widetilde{O}(h_0 R_0 B^2) = O(\Delta_1 \Delta_0^{5/2+\epsilon})$, which proves the following result.

**Theorem 2.7.** *On input a quartic CM-field $K$, Algorithm 2.5 runs in time $O(\Delta_1 \Delta_0^{5/2+\epsilon})$.* □

## 2.4 Generalization of Spallek's formula

Spallek, in her thesis [79], gave a formula for the period matrices of a complete set of representatives of the isomorphism classes of abelian surfaces with CM by a given primitive quartic CM-field $K$ of which the real quadratic subfield $K_0$ has class number one. This formula has been the method of choice of other authors and even made it into a textbook [27, 97]. The theory of the Section I.5.3 allows us to simplify Spallek's results and to generalize them to arbitrary primitive quartic CM-fields.

Let $K$ be a primitive quartic CM-field with real quadratic subfield $K_0$ and let $\omega \in K_0$ be such that $\mathcal{O}_{K_0} = \mathbf{Z}[\omega]$.

**Lemma 2.8.** *Suppose that $z \in K$ is such that $z\mathcal{O}_{K_0} + \mathcal{O}_{K_0}$ is an $\mathcal{O}_K$-ideal. Let $\phi_1, \phi_2$ be the embeddings of $K$ into $\mathbf{C}$ given by $\phi_1\omega > \phi_2\omega$ and $\operatorname{Im}\phi_1(z) > 0 > \operatorname{Im}\phi_2(z)$. Then the abelian variety corresponding to the pair $(z, \mathfrak{b})$ has a period matrix*

$$Z_z = \sum_{i=1}^{2} \phi_i\Big(z\delta^{-1}\begin{pmatrix} \omega^2 & \omega \\ \omega & 1 \end{pmatrix}\Big) \in \mathcal{H}_2.$$

*Proof.* Choose $b_1 = \omega$ and $b_2 = 1$ in Theorem II.4.3. □

**Theorem 2.9.** *Let $K$ be a primitive quartic CM-field. A complete set of representatives for the isomorphism classes of abelian varieties over $\mathbf{C}$ with CM by $\mathcal{O}_K$ can be obtained as follows.*

1. *Let $\Phi = \{\phi_1, \phi_2\}$ be a CM-type of $K$.*
2. *Let $\epsilon \in \mathcal{O}_{K_0}^*$ be such that $\langle -1\rangle \times \langle \epsilon\rangle$ has odd index in $\mathcal{O}_{K_0}^*$.*
3. *Let $\mathcal{K}' \subset K$ be such that $\{z\mathcal{O}_{K_0} + \mathcal{O}_{K_0} : z \in \mathcal{K}'\}$ is a complete set of representatives of the ideal classes of $K$ that contain an ideal of the form $z\mathcal{O}_{K_0} + \mathcal{O}_{K_0}$.*
4. *Let $\mathcal{K} = \pm\mathcal{K}' \cup \pm\epsilon\mathcal{K}'$.*
5. *If $K$ is cyclic Galois, return*

$$\{Z_z \mid z \in \mathcal{K},\ \operatorname{Im}\phi_1 z > 0 > \operatorname{Im}\phi_2 z\}.$$

*6. If $K$ is non-Galois, return*

$$\{Z_z \mid z \in \mathcal{K},\ \operatorname{Im} \phi_1 z > 0\}.$$

*Proof.* Algorithm II.3.1 gives a complete set of representatives of the isomorphism classes of principally polarized abelian varieties over $\mathbf{C}$ with CM by $\mathcal{O}_K$. Theorems I.5.8 and I.5.9 show that the ideal classes $\mathfrak{a}$ of step 4 of Algorithm II.3.1 are exactly the ones that contain a representative of the form $z\mathcal{O}_{K_0} + \mathcal{O}_{K_0}$. Moreover, $\xi = (z - \overline{z})^{-1}\delta^{-1}$ gives a choice of $\xi$ as in step 4 of Algorithm II.3.1.

We use Corollary II.3.4 to compute $\mathcal{O}_{K_0}^*/N_{K/K_0}(\mathcal{O}_K^*)$ (which consists of the classes of $\pm 1$ and $\pm\epsilon$) and Lemma I.3.4 to compute a complete set of representatives for the equivalence classes of CM-types ($\{\Phi\}$ if $K$ is cyclic Galois and $\{\Phi, \{\phi_1, \overline{\phi_2}\}\}$ if $K$ is non-Galois).

Multiplication of $\xi$ by $u \in \mathcal{O}_{K_0}^*$ corresponds exactly to multiplication of $z$ by $u^{-1}$, so $\mathcal{K}$ corresponds exactly to the set of triples $(\mathfrak{a}, \xi, u)$ of step 5 of Algorithm II.3.1. Steps 5 and 6 are the same as step 6 of Algorithm II.3.1. □

# Appendix 3. Experimental results

Abstract. *We show that our choice of absolute Igusa invariants leads to smaller class polynomials experimentally. We also study how the denominator and numerator of the coefficients of class polynomials grow with the discriminant of the CM-field.*

## 3.1 Good absolute Igusa invariants

We computed Igusa class polynomials of over a thousand fields in the ECHIDNA database [50] for the 13 invariants listed in Table 2.

| | | | |
|---|---|---|---|
| $i_1$ | = | $I_4 I_6'/I_{10}$ | as in Chapter II |
| $i_2$ | = | $I_2 I_4^2/I_{10}$ | as in Chapter II |
| $i_3$ | = | $I_4^5/I_{10}^2$ | as in Chapter II |
| $i_4$ | = | $I_4 I_6/I_{10}$ | the invariant $i_1$ in ECHIDNA [50] |
| $i_5$ | = | $I_2^5/I_{10}$ | $2^3$ times Spallek's $j_1$ (see [79]) |
| $i_6$ | = | $I_2^3 I_4/I_{10}$ | ECHIDNA's $i_2$; $2^{-1}$ times Spallek's $j_2$ |
| $i_7$ | = | $I_2^3 I_6/I_{10}$ | ECHIDNA's $i_3$; $2^{-3}$ times Spallek's $j_3$ |
| $i_8$ | = | $I_6'/(I_2 I_4)$ | |
| $i_9$ | = | $I_6'^2/I_4^3$ | |
| $i_{10}$ | = | $I_2 I_6'/I_4^2$ | |
| $i_{11}$ | = | $I_6'^2/(I_2 I_{10})$ | |
| $i_{12}$ | = | $I_4^3/(I_2 I_{10})$ | |
| $i_{13}$ | = | $I_4/I_2^2$ | an invariant used by van Wamelen [89] |

Table 2: Table of Igusa invariants

For each class polynomial $H$, we computed the coefficient with the largest absolute value of the primitive integral polynomial $dH$, where $d$

is the denominator of $H$. Figures 2–4 show how these coefficients grow relative to the coefficients for $i_4$. Our invariants $i_1$, $i_2$, $i_3$ from Chapter II are yellow, those of Spallek ($i_5$, $i_6$, $i_7$) are red, and ECHIDNA's $i_4$ is blue. The purple and green invariants have denominators that are not of the form $I_{10}^k$.

We computed a least-squares fitting linear map, which is shown in Table 3 and Figures 2–4.

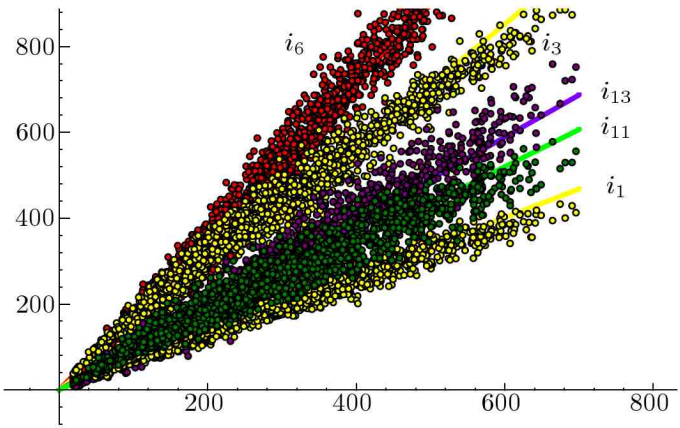



Figure 2: The logarithm of the largest coefficient of the integral Igusa class polynomial for the given invariant (on the vertical axis) relative to the logarithm of the largest coefficient of the polynomial for $i_4$ (on the horizontal axis). We used SAGE [70] to draw this graph and the others in this section.

Table 3 shows that, out of the invariants that we tried, the best invariant is $i_1$.

It is followed by six invariants $i_8$, $i_9$, $i_{10}$, $i_{11}$, $i_{12}$, and $i_{13}$ that are not elements of the ring $\mathbf{Q}[I_2, I_4, I_6, I_{10}^{-1}]$, but of its fraction field. These are invariants that we disregarded in Chapter II as they are not guaranteed to be finite. In practice, they are always finite, and the algorithm of Chapter II can be made to work for these invariants. The table shows that these invariants yield good class polynomials $H_n$.

We computed the (interpolating) class polynomials $\widehat{H}_n$ for the triple $i_1$, $i_8$, $i_9$ and the field $K = \mathbf{Q}[X]/(X^4 + 450X^2 + 28153)$ with class number 14. This yielded class polynomials $\widehat{H}_2$ and $\widehat{H}_3$ that are much

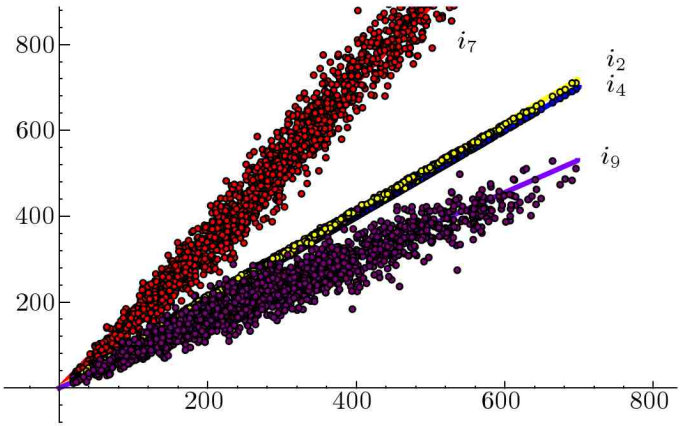



Figure 3: The largest coefficient of the Igusa class polynomial for the given invariant relative to the largest coefficient of the polynomial for $i_4$.

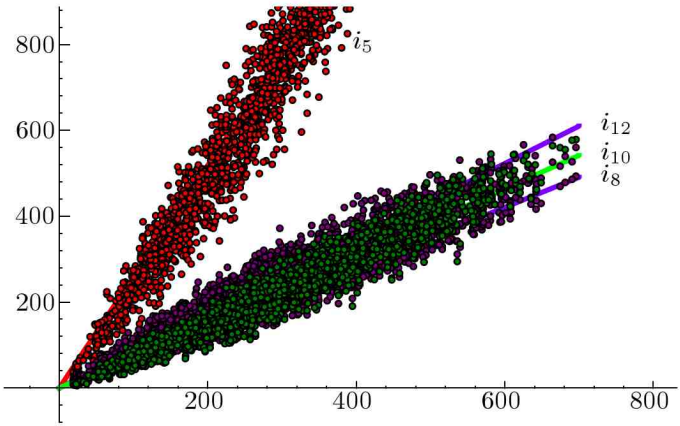



Figure 4: The largest coefficient of the Igusa class polynomial for the given invariant relative to the largest coefficient of the polynomial for $i_4$.

| | | | | | | |
|---|---|---|---|---|---|---|
| $i_1$ | = | $I_4 I_6'/I_{10}$ | = | $h_4 h_6/h_{10}$ | Chapter II | 0.6686 |
| $i_8$ | = | $I_6'/(I_2 I_4)$ | = | $h_6 h_{10}/(h_4 h_{12})$ | | 0.7012 |
| $i_9$ | = | $I_6'^2/I_4^3$ | = | $h_6^2/h_4^3$ | | 0.7590 |
| $i_{10}$ | = | $I_2 I_6'/I_4^2$ | = | $h_6 h_{12}/(h_4^2 h_{10})$ | | 0.7740 |
| $i_{11}$ | = | $I_6'^2/(I_2 I_{10})$ | = | $h_6^2/h_{12}$ | | 0.8666 |
| $i_{12}$ | = | $I_4^3/(I_2 I_{10})$ | = | $h_4^3/h_{12}$ | | 0.8716 |
| $i_{13}$ | = | $I_4/I_2^2$ | = | $h_4 h_{10}^2/h_{12}^2$ | | 0.9818 |
| $i_4$ | = | $I_4 I_6/I_{10}$ | = | $h_4 h_{16}/h_{10}^2$ | ECHIDNA | 1 |
| $i_2$ | = | $I_2 I_4^2/I_{10}$ | = | $h_4^2 h_{12}/h_{10}^2$ | Chapter II | 1.0294 |
| $i_3$ | = | $I_4^5/I_{10}^2$ | = | $h_4^5/h_{10}^2$ | Chapter II | 1.4203 |
| $i_7$ | = | $I_2^2 I_6/I_{10}$ | = | $h_{12}^2 h_{16}/h_{10}^4$ | Spallek | 1.7799 |
| $i_6$ | = | $I_2^3 I_4/I_{10}$ | = | $h_4 h_{12}^3/h_{10}^4$ | Spallek | 1.7949 |
| $i_5$ | = | $I_2^5/I_{10}$ | = | $h_{12}^5/h_{10}^6$ | Spallek | 2.5921 |

Table 3: The invariants sorted by the slopes of the lines in Figures 2–4.

*larger* instead of smaller than the class polynomials for the invariants $i_1$, $i_2$, $i_3$.

A possible explanation of this phenomenon is the fact that the denominators of the polynomials $\widehat{H}_n$ are divisible by the prime divisors of both the denominator of the first invariant and the $n$-th invariant. To fix this, one would need invariants that have the same denominator modular form. We therefore also computed the Igusa class polynomials $H_1$, $\widehat{H}_2$, and $\widehat{H}_3$ for the same field also for the triple $i_8$, $i_{11}$, and $i_{12}$, which shares the denominator $h_4 h_{12}$. However, the class polynomials for $i_1$, $i_2$, and $i_3$ are still smaller. As we have not tested all quotients of modular forms of small height, there may exist invariants that are better than $i_1$, $i_2$, $i_3$.

After $i_8, \ldots, i_{13}$, the next two invariants $i_4$ and $i_2$ are roughly of equal size. As the triple of invariants $(i_1, i_2, i_4)$ is algebraically (in fact, linearly) dependent, this triple does not determine a point in the three-dimensional moduli space. The next invariant is $i_3$, which explains why we chose the triple $(i_1, i_2, i_3)$ (up to constant factors) as our absolute Igusa invariants in Chapter II.

The invariants $i_5$, $i_6$, $i_7$ are much used in the computational literature (see [17, 97, 88] and up to constants also Spallek [79]). This is for historical reasons rather than efficiency reasons, as Spallek based them on the first three of 10 lexicographically ordered invariants of Igusa [45]. Table 3 shows that they yield class polynomials that are larger than the

class polynomials for $i_1$, $i_2$, and $i_3$.

We save only a constant factor in the bit sizes of the polynomials by using our invariants instead of Spallek's. However, as with the use of *class invariants* for elliptic curves such as *Weber functions* (see e.g. Schertz [71]), a constant factor makes a big difference in practice for these large polynomials.

**Example 3.10.** We took the example $K = \mathbf{Q}[X]/(X^4 + 15X^2 + 55)$ from [97]. There, the invariants $i_5$, $i_6$, and $i_7$ are used, and the minimal polynomial of $i_5$ is not printed due to its size. The minimal polynomial of $i_6$ takes up a lot less space, and is given in Figure 5. The minimal polynomial of $i_7$ is about as large as the one for $i_6$.

$$
\begin{aligned}
&3^{12}11^{14}13^{16}X^8 \\
&-2777909653672665381895067460192197189029239604510740000 0X^7 \\
&+3467200369701648645206339996478360530210019317723277316023975000000 00X^6 \\
&-3239358921736475318707092123999841732942740721735230943046057501508750000000000000X^5 \\
&-2093721883795019411322012764576680703208429855295129262962399815659466406250000 00 \\
&0000000X^4 \\
&+6032886253404225073888875910817726659676479347407382050398247624640325195312500 00 \\
&00000000000000X^3 \\
&-2340167052536858943805619476102801375431918749314028230572028585795131939697265 62 \\
&5000000000000000000000X^2 \\
&+1053473453098145151468621039011601503497253830709038795204774581354138945007324 21 \\
&8750000000000000000000000000X \\
&-1271668372760513962565290807560235110248194311521869842647053908811859044551849 36 \\
&52343750000000 \in \mathbf{Z}[X].
\end{aligned}
$$

Figure 5: A constant times the minimal polynomial of $i_6(C)$ for a curve $C$ with CM by the maximal order of $K = \mathbf{Q}[X]/(X^4 + 15X^2 + 55)$ as in [97].

With our invariants of Chapter II, the complete output of the class polynomial computation is given in Figure 6. Note that each of the polynomials is a lot smaller than the one in Figure 5.

## 3.2 Asymptotics of bit sizes

For thousands of CM-fields in the ECHIDNA database, we took the largest coefficient $c$ of the primitive integral polynomial $dH$, where $H$ is the class polynomial $H$ for the invariant $i_4$, and $d$ is the denominator of $H$.

We used SAGE [70] to find a least-square fitting surface for the set of points

$$(\log \Delta_0, \log \Delta_1, \log \log c) \in \mathbf{R}^3,$$

$$
\begin{aligned}
13^4 H_1 =& 28561X^8 - 63024286247286000X^7 + \\
& 5089603200935139203672250000X^6 - \\
& 491194385305230285106635375000000X^5 + \\
& 150708240517912053562313289296875000000X^4 - \\
& 16186136281764062071284438363281250000000000X^3 + \\
& 3078576886855075275041917745361328125000000000X^2 + \\
& 689204580516602397785625617065429687500000000000X - \\
& 110030479233737207241982326107025146484375000000000
\end{aligned}
$$

$$
\begin{aligned}
11^2 13^6 \widetilde{H}_2 =& 90966043775189898900000X^7 - \\
& 8453896932952685422851138300000000X^6 + \\
& 4810669345723139916396063321918750000000X^5 - \\
& 2177906607073667086888889343652718750000000000X^4 + \\
& 281267072106125538087082967961134179687500000000000X^3 - \\
& 58120060856092296588992618536371679687500000000000000X^2 - \\
& 12480609623516533259889607271847381591796875000000000000X \\
& + 215389197036958387031899522270161437988281250000000000000000
\end{aligned}
$$

$$
\begin{aligned}
11^2 13^6 \widetilde{H}_3 =& 10544496589569296093552499375000000X^7 - \\
& 9187900714185758782843682611812206250000000000X^6 + \\
& 886718601168575390202949228741227826953125000000000X^5 - \\
& 272062980655758803935983328396874486654296875000000000000X^4 + \\
& 29219693869772398316627802410434325592736816406250000000000000X^3 - \\
& 5557538520725201105261803647250481764892578125000000000000000000X^2 - \\
& 1244172594273819471769874031305214335557937622070312500000000000000X + \\
& 19863029194037092925339961228093767220783233642578125000000000000000
\end{aligned}
$$

Figure 6: The Igusa class polynomials for the CM-field $K = \mathbf{Q}[X]/(X^4 + 15X^2 + 55)$ as defined in Chapter II.

and found the approximate relation

$$\log\log c \approx 0.53 \log \Delta_0 + 0.58 \log \Delta_1 + 0.35.$$

From this, we conclude that the bit size $\log_2 c$ of $c$ seems to grow roughly like $(\Delta_0\Delta_1)^{1/2}$, just like the degree of $H$ (see Section II.8). We plotted $\log\log c$ in terms of $\log\log(\Delta_0\Delta_1)$ in Figure 7, which supports this estimate for the growth.

If the bit sizes of the coefficients grow like $(\Delta_0\Delta_1)^{1/2}$, then the bit size of $H$ grows like $\Delta_0\Delta_1$. As we used only relatively small examples, this may not be the correct asymptotic growth of the Igusa class polynomials, but it should give a good indication for the accessible examples.

The gap between the proven bound in the runtime and the much smaller expected size of the class polynomials is explained by

1. the fact that the denominator bounds of Goren and Lauter in Section II.9 are not optimal,

2. the fact that our bounds in Section II.6 are not optimal, and

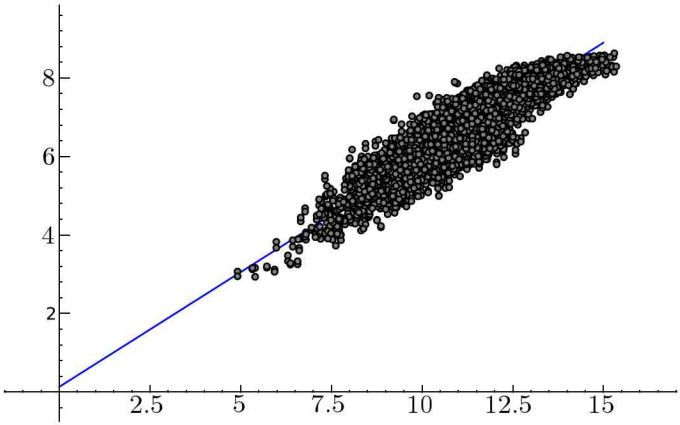



Figure 7: The double logarithm $\log\log c$ of the largest coefficient $c$ of the Igusa class polynomial for $i_4$ as a function of $\log(\Delta_0\Delta_1)$. The slope of the line is 0.58.

3. the fact that we use a quasi-quadratic method for computing theta constants in Section II.7.

# Bibliography


[1] A. Oliver L. Atkin and François Morain. Elliptic curves and primality proving. *Mathematics of Computation*, 61(203):29–68, 1993. `http://www.inria.fr/rrrt/rr-1256.html`. (cited on page 136)

[2] Juliana Belding, Reinier Bröker, Andreas Enge, and Kristin Lauter. Computing Hilbert class polynomials. In *Algorithmic Number Theory – ANTS-VIII (Banff, 2008)*, volume 5011 of *LNCS*, pages 282–295. Springer, 2008. (cited on page 39)

[3] Daniel J. Bernstein. Fast multiplication and its applications. In J. Buhler and P. Stevenhagen, editors, *Surveys in Algorithmic Number Theory* [11], pages 325–384, 2008. (cited on page 72)

[4] Christina Birkenhake and Herbert Lange. *Complex abelian varieties*, volume 302 of *Grundlehren der mathematischen Wissenschaften*. Springer, second edition, 2004. The first part of this book appeared as [53]. (cited on pages 23, 28, 29, and 172)

[5] Oskar Bolza. Darstellung der rationalen ganzen Invarianten der Binärform sechsten Grades durch die Nullwerthe der zugehörigen $\vartheta$-Functionen. *Math. Ann.*, 30(4):478–495, 1887. (cited on page 69)

[6] Dan Boneh, Eu-Jin Goh, and Kobbi Nissim. Evaluating 2-DNF formulas on ciphertexts. In *TCC '05*, volume 3378 of *Lecture Notes in Computer Science*, pages 325–341. Springer, 2005. (cited on page 112)

[7] Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system I: The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993). (cited on pages 95, 97, and 99)

[8] Jan Hendrik Bruinier and Tonghai Yang. CM-values of Hilbert modular functions. *Invent. Math.*, 163(2):229–288, 2006. (cited on pages 77 and 82)

[9] Johannes Buchmann and Hendrik W. Lenstra, Jr. Approximating rings of integers in number fields. *Journal de Théorie des Nombres de Bordeaux*, 6:221–260, 1994. (cited on pages 48 and 87)

[10] Johannes Buchmann, Christoph Thiel, and Hugh Williams. Short representation of quadratic integers. In *Computational algebra and number theory (Sydney, 1992)*, volume 325 of *Math. Appl.*, pages 159–185. Kluwer Acad. Publ., 1995. (cited on page 155)

[11] Joe P. Buhler and Peter Stevenhagen, editors. *Surveys in Algorithmic Number Theory*, volume 44 of *MSRI Publications*. Cambridge University Press, 2008. (cited on pages 167, 168, 172, 174, and 175)

[12] Gabriel Cardona and Jordi Quer. Field of moduli and field of definition for curves of genus 2. In *Computational aspects of algebraic curves*, volume 13 of *Lecture Notes Ser. Comput.*, pages 71–83. World Scientific, 2005. (cited on pages 43 and 102)

[13] Robert Carls, David Kohel, and David Lubicz. Higher-dimensional 3-adic CM construction. *J. Algebra*, 319(3):971–1006, 2008. (cited on page 40)

[14] Robert Carls and David Lubicz. A $p$-adic quasi-quadratic time point counting algorithm. *Int. Math. Res. Not. IMRN*, (4):698–735, 2009. (cited on page 40)

[15] Alfred Clebsch. Zur Theorie der binären algebraischen Formen. *Math. Ann.*, 3(2):265–267, 1870. (cited on page 42)

[16] Henri Cohen. *A Course in Computational Algebraic Number Theory*, volume 138 of *Graduate Texts in Mathematics*. Springer, 1993. (cited on page 131)

[17] Henri Cohen, Gerhard Frey, Roberto Avanzi, Christophe Doche, Tanja Lange, Kim Nguyen, and Frederik Vercauteren, editors. *Handbook of elliptic and hyperelliptic curve cryptography*. Chapman & Hall/CRC, Boca Raton, FL, 2006. (cited on pages 162, 169, and 170)

[18] Henri Cohen and Peter Stevenhagen. Computational class field theory. In J. Buhler and P. Stevenhagen, editors, *Surveys in Algorithmic Number Theory* [11], pages 497–534, 2008. (cited on page 18)

[19] David A. Cox. *Primes of the form $x^2 + ny^2$*. John Wiley & Sons, 1989. (cited on page 190)

[20] Régis Dupont. *Moyenne arithmético-géométrique, suites de Borchardt et applications.* PhD thesis, École Polytechnique, 2006. `http://www.lix.polytechnique.fr/Labo/Regis.Dupont/these_soutenance.pdf`. (cited on pages 67, 69, 70, 71, 74, and 90)

[21] Kirsten Eisenträger and Kristin Lauter. A CRT algorithm for constructing genus 2 curves over finite fields. To appear in *Arithmetic, Geometry and Coding Theory, AGCT-10* (Marseille, 2005), 2005. (cited on pages 40 and 137)

[22] Andreas Enge. The complexity of class polynomial computation via floating point approximations. *Mathematics of Computation*, 78(266):1089–1107, 2009. (cited on page 39)

[23] Andreas Enge and François Morain. Fast decomposition of polynomials with known Galois group. In *Applied algebra, algebraic algorithms and error-correcting codes (Toulouse, 2003)*, volume 2643 of *Lecture Notes in Comput. Sci.*, pages 254–264, Berlin, 2003. Springer. (cited on pages 44 and 88)

[24] David Freeman. Constructing pairing-friendly genus 2 curves over prime fields with ordinary Jacobians. In *Pairing-Based Cryptography – Pairing 2007*, volume 4575 of *Lecture Notes in Computer Science*, pages 152– 176, Berlin, 2007. Springer-Verlag. (cited on page 124)

[25] David Freeman, Michael Scott, and Edlyn Teske. A taxonomy of pairing-friendly elliptic curves. Cryptology ePrint Archive, Report 2006/372, 2006. `http://eprint.iacr.org/2006/372`. (cited on page 109)

[26] David Freeman, Peter Stevenhagen, and Marco Streng. Abelian varieties with prescribed embedding degree. In *Algorithmic Number Theory, 8th International Symposium, ANTS-VIII, Banff, Canada, May 17-22, 2008, Proceedings* [87], pages 60–73, 2008. Appears as Chapter IV in this thesis. (cited on pages 15, 100, 105, 124, 134, 135, and 136)

[27] Gerhard Frey and Tanja Lange. Complex multiplication. In *Handbook of elliptic and hyperelliptic curve cryptography* [17], pages 455–473. Chapman & Hall/CRC, 2006. (cited on pages 41, 70, 136, and 157)

[28] Gerhard Frey and Tanja Lange. Varieties over special fields. In *Handbook of elliptic and hyperelliptic curve cryptography* [17], pages 87–113. Chapman & Hall/CRC, 2006. (cited on page 43)

[29] Gerhard Frey and Hans-Georg Rück. A remark concerning $m$-divisibility and the discrete logarithm in the divisor class group of curves. *Mathematics of Computation*, 62:865–874, 1994. (cited on page 106)

[30] Steven Galbraith. Supersingular curves in cryptography. In *ASIACRYPT '01*, volume 2248 of *Lecture Notes in Computer Science*, pages 495–513. Springer, 2001. (cited on page 107)

[31] Pierrick Gaudry, Thomas Houtmann, David Kohel, Christophe Ritzenthaler, and Annegret Weng. The $p$-adic CM-method for genus 2, 2005. arXiv:math/0503148, see also [32]. (cited on pages 40 and 170)

[32] Pierrick Gaudry, Thomas Houtmann, David Kohel, Christophe Ritzenthaler, and Annegret Weng. The 2-adic CM method for genus 2 curves with application to cryptography. In *Advances in Cryptology – ASIACRYPT 2006*, volume 4284 of *Lecture Notes in Computer Science*, pages 114–129, Berlin, 2006. Springer-Verlag. see also [31]. (cited on pages 40, 44, 137, and 170)

[33] Josep González. On the $p$-rank of an abelian variety and its endomorphism algebra. *Pub. Math.*, 42(1):119–130, 1998. (cited on pages 125, 126, and 127)

[34] Eyal Z. Goren. On certain reduction problems concerning abelian surfaces. *manuscripta mathematica*, 94(1):33–43, 1997. (cited on pages 78, 99, and 125)

[35] Eyal Z. Goren and Kristin Lauter. Class invariants for quartic CM fields. *Annales de l'Institut Fourier*, 57(2):457–480, 2007. (cited on pages 40, 41, 43, 76, 77, and 78)

[36] Eyal Z. Goren and Kristin Lauter. Genus 2 curves with complex multiplication. arXiv:1003.4759v1, 2010. (cited on pages 40, 41, 76, 77, 78, and 79)

[37] Erhard Gottschling. Die Randflächen des Fundamentalbereiches der Modulgruppe. *Math. Annalen*, 138:103–124, 1959. (cited on pages 56 and 63)

[38] Guillaume Hanrot and François Morain. Solvability by radicals from an algorithmic point of view. In *Proceedings of the 2001 International Symposium on Symbolic and Algebraic Computation*, pages 175–182 (electronic), New York, 2001. ACM. (cited on page 44)

[39] Godfrey Harold Hardy and Edward Maitland Wright. *An Introduction to the Theory of Numbers*. Oxford University Press, 1938. (cited on pages 132 and 155)

[40] Erich Hecke. *Vorlesungen über die Theorie der algebraischen Zahlen*. Chelsea Publishing Co., Bronx, N.Y., 1970. Second edition of the 1923 original, with an index. (cited on page 44)

[41] Marc Hindry and Joseph H. Silverman. *Diophantine geometry*, volume 201 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2000. An introduction. (cited on page 29)

[42] Laura Hitt. On the minimal embedding field. In *Pairing-Based Cryptography – Pairing 2007*, volume 4575 of *Lecture Notes in Computer Science*, pages 294–301. Springer-Verlag, 2007. (cited on page 136)

[43] Laura Hitt O'Connor, Gary McGuire, Michael Naehrig, and Marco Streng. A CM construction for curves of genus 2 with $p$-rank 1. To be published by Journal of Number Theory, arXiv:0811.3434v2, appears as Chapter V in this thesis, 2008. (cited on pages 15 and 123)

[44] Taira Honda. Isogeny classes of abelian varieties over finite fields. *J. Math. Soc. Japan*, 20:83–95, 1968. (cited on page 124)

[45] Jun-Ichi Igusa. Arithmetic variety of moduli for genus two. *Annals of Mathematics*, 72(3):612–649, 1960. (cited on pages 42, 43, 92, 136, 138, and 162)

[46] Jun-Ichi Igusa. On siegel modular forms of genus two. *American Journal of Mathematics*, 84(1):175–200, 1962. (cited on page 69)

[47] Jun-Ichi Igusa. Modular forms and projective invariants. *American Journal of Mathematics*, 89(3):817–855, 1967. `http://www.jstor.org/stable/2373243`. (cited on pages 69 and 150)

[48] Helmut Klingen. *Introductory lectures on Siegel modular forms*, volume 20 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 1990. (cited on pages 57, 58, 59, and 71)

[49] Ann Hibner Koblitz, Neal Koblitz, and Alfred Menezes. Elliptic curve cryptography: The serpentine course of a paradigm shift. Cryptology ePrint Archive, Report 2008/390, 2008. To appear in Journal of Number Theory, `http://eprint.iacr.org/2008/390`.

[50] David Kohel et al. ECHIDNA algorithms for algebra and geometry experimentation. `http://echidna.maths.usyd.edu.au/~kohel/dbs/complex_multiplication2.html`. (cited on pages 43, 82, 93, 137, 141, and 159)

[51] Kenji Koike and Annegret Weng. Construction of CM Picard curves. *Mathematics of Computation*, 74:499–518, 2004. (cited on page 119)

[52] Serge Lang. *Complex Multiplication*, volume 255 of *Grundlehren der mathematischen Wissenschaften*. Springer, 1983. (cited on pages 19, 21, 22, 25, 30, 32, 34, and 95)

[53] Herbert Lange and Christina Birkenhake. *Complex abelian varieties*, volume 302 of *Grundlehren der mathematischen Wissenschaften*. Springer, 1992. reappeared in [4]. (cited on page 167)

[54] Kristin Lauter. Primes in the denominators of Igusa class polynomials. 2003. (cited on pages 77 and 82)

[55] Arjen K. Lenstra, Hendrik W. Lenstra, Jr., and László Lovász. Factoring polynomials with rational coefficients. *Math. Ann.*, 261(4):515–534, 1982. (cited on page 95)

[56] Hendrik W. Lenstra, Jr. On the calculation of regulators and class numbers of quadratic fields. In *Journées Arithmétiques 1980*, pages 123–150. Cambridge University Press, 1982. (cited on pages 153, 154, and 155)

[57] Hendrik W. Lenstra, Jr. Lattices. In J. Buhler and P. Stevenhagen, editors, *Surveys in Algorithmic Number Theory* [11], pages 127–181, 2008. (cited on pages 47, 50, 55, 86, and 95)

[58] Stéphane Louboutin. Explicit lower bounds for residues at $s = 1$ of Dedekind zeta functions and relative class numbers of CM-fields. *Trans. Amer. Math. Soc.*, 355(8):3079–3098 (electronic), 2003. (cited on page 76)

[59] Daniel Maisner and Enric Nart. Abelian surfaces over finite fields as Jacobians. *Experiment. Math.*, 11(3):321–337, 2002. With an appendix by Everett W. Howe. (cited on page 127)

[60] Alfred Menezes, Tatsuaki Okamoto, and Scott A. Vanstone. Reducing elliptic curve logarithms to logarithms in a finite field. *IEEE Transactions on Information Theory*, 39:1639–1646, 1993. (cited on page 106)

[61] Jean-François Mestre. Construction de courbes de genre 2 à partir de leurs modules. In *Effective methods in algebraic geometry (Castiglioncello, 1990)*, volume 94 of *Progr. Math.*, pages 313–334, Boston, MA, 1991. Birkhäuser Boston. (cited on pages 43, 99, and 136)

[62] James S. Milne. Abelian varieties. In *Arithmetic Geometry*, pages 103–150, New York, 1986. Springer. (cited on page 23)

[63] James S. Milne. Jacobian varieties. In *Arithmetic Geometry*, pages 167–212, New York, 1986. Springer. (cited on page 28)

[64] James S. Milne. Complex multiplication. Version 0.00. Available at `http://www.jmilne.org/math/`, 2006. (cited on pages 19, 21, 22, 30, 34, and 95)

[65] David Mumford. *Tata lectures on theta II*, volume 43 of *Progress in Mathematics*. Birkhäuser, 1984. (cited on page 69)

[66] Jürgen Neukirch. *Algebraische Zahlentheorie*. Springer, 1992. (cited on pages 27, 129, and 140)

[67] Kenny Paterson. Cryptography from pairings. In I.F. Blake, G. Seroussi, and N.P. Smart, editors, *Advances in Elliptic Curve Cryptography*, pages 215–251. Cambridge University Press, 2005. (cited on page 106)

[68] H.L. Resnikoff and R.L. Saldaña. Some properties of Fourier coefficients of Eisenstein series of degree two. *J. Reine Angew. Math.*, 265:90–109, 1974. (cited on page 150)

[69] Karl Rubin and Alice Silverberg. Supersingular abelian varieties in cryptology. In *Proceedings of the 22nd Annual International Cryptology Conference on Advances in Cryptology*, volume 2442 of *Lecture Notes In Computer Science*, pages 336–353, 2002. (cited on pages 107 and 124)

[70] SAGE. SAGE mathematics software, version 4.0.1. `http://www.sagemath.org/`. (cited on pages 4, 160, and 163)

[71] Reinhard Schertz. Die singulären Werte der Weberschen Funktionen $\mathfrak{f}$, $\mathfrak{f}_1$, $\mathfrak{f}_2$, $\gamma_2$, $\gamma_3$. *J. Reine Angew. Math.*, 286/287:46–74, 1976. (cited on page 163)

[72] René Schoof. Elliptic curves over finite fields and the computation of square roots mod $p$. *Math. Comp.*, 44(170):483–494, 1985.

[73] René Schoof. Computing Arakelov class groups. In J. Buhler and P. Stevenhagen, editors, *Surveys in Algorithmic Number Theory* [11], pages 447–495, 2008. (cited on page 47)

[74] Daniel Shanks. Class number, a theory of factorization, and genera. In *1969 Number Theory Institute (Proc. Sympos. Pure Math., Vol. XX, State Univ. New York, Stony Brook, N.Y., 1969)*, pages 415–440, Providence, R.I., 1971. Amer. Math. Soc. (cited on page 153)

[75] Daniel Shanks. The infrastructure of a real quadratic field and its applications. In *Proceedings of the Number Theory Conference (Univ. Colorado, Boulder, Colo., 1972)*, pages 217–224, Boulder, Colo., 1972. Univ. Colorado. (cited on page 153)

[76] Goro Shimura. On the class-fields obtained by complex multiplication of abelian varieties. *Osaka Math. J.*, 14:33–44, 1962. (cited on pages 14, 17, 35, and 36)

[77] Goro Shimura. *Abelian Varieties with Complex Multiplication and Modular Functions*. Princeton University Press, 1998. Sections 1–16 essentially appeared before in [78]. (cited on pages 110, 138, and 174)

[78] Goro Shimura and Yutaka Taniyama. *Complex multiplication of abelian varieties and its applications to number theory*, volume 6 of *Publications of the Mathematical Society of Japan*. The Mathematical Society of Japan, Tokyo, 1961. Sections 1–16 essentially reappeared in [77]. (cited on pages 18, 19, 20, 21, 22, 24, 25, 29, 30, 31, 32, 34, 98, 124, 126, 136, 138, 139, and 174)

[79] Anne-Monika Spallek. *Kurven vom Geschlecht* 2 *und ihre Anwendung in Public-Key-Kryptosystemen*. PhD thesis, Institut für Experimentelle Mathematik, Universität GH Essen, 1994. `http://www.uni-due.de/zahlentheorie/theses_de.shtml`. (cited on pages 14, 15, 24, 40, 41, 43, 69, 124, 137, 157, 159, and 162)

[80] Peter Stevenhagen. Hilbert's 12th problem, complex multiplication and Shimura reciprocity. In *Class field theory – its centenary and*

*prospect (Tokyo, 1998)*, volume 30 of *Adv. Stud. Pure Math.*, pages 161–176. Math. Soc. Japan, Tokyo, 2001.

[81] Peter Stevenhagen. The arithmetic of number rings. In J. Buhler and P. Stevenhagen, editors, *Surveys in Algorithmic Number Theory* [11], 2008. (cited on page 142)

[82] Marco Streng. Computing Igusa class polynomials. arXiv:0903.4766, appears as Chapter II in this thesis, 2008. (cited on page 137)

[83] Marco Streng. Divisibility sequences for elliptic curves with complex multiplication. *Algebra & Number Theory*, 2(2):183–208, 2008.

[84] John Tate. Classes d'isogénie des variétés abéliennes sur un corps fini (d'après T. Honda). *Sémin. Bourbaki 1968/69, No.352*, pages 95–110, 1971. (cited on pages 98, 106, 108, 117, 124, and 126)

[85] Carl Johannes Thomae. Beitrag zur Bestimmung von $\vartheta(0, \cdots, 0)$ durch die Klassenmoduln algebraischer Funktionen. *J. reine angew. Math.*, 71:201–222, 1870. (cited on page 69)

[86] Gerard van der Geer. *Hilbert modular surfaces*, volume 16 of *Ergebnisse der Mathematik und ihrer Grenzgebiete (3)*. Springer, Berlin, 1988. (cited on pages 67, 152, and 153)

[87] Alfred J. van der Poorten and Andreas Stein, editors. *Algorithmic Number Theory, 8th International Symposium, ANTS-VIII, Banff, Canada, May 17-22, 2008, Proceedings*, volume 5011 of *Lecture Notes in Computer Science*. Springer-Verlag, 2008. (cited on page 169)

[88] Paul van Wamelen. Examples of genus two CM curves defined over the rationals. *Mathematics of Computation*, 68(225):307–320, 1999. (cited on pages 14, 24, 25, 26, 40, 41, 43, 46, 120, 137, and 162)

[89] Paul van Wamelen. Computing with the analytic Jacobian of a genus 2 curve. In *Discovering mathematics with Magma*, volume 19 of *Algorithms Comput. Math.*, pages 117–135, Berlin, 2006. Springer. (cited on page 159)

[90] Joachim von zur Gathen and Jürgen Gerhard. *Modern computer algebra*. Cambridge University Press, Cambridge, second edition, 2003. (cited on pages 83, 85, 86, and 88)

[91] Lawrence C. Washington. *Introduction to Cyclotomic Fields*. Number 83 in Graduate Texts in Mathematics. Springer, 1982. (cited on page 25)

[92] William C. Waterhouse. Abelian varieties over finite fields. *Ann. Sci. École Norm. Sup. (4)*, 2:521–560, 1969. (cited on page 108)

[93] Heinrich Weber. *Algebraische Zahlen*, volume 3 of *Lehrbuch der Algebra*. Braunschweig, Friedrich Vieweg, 1908. (cited on page 39)

[94] André Weil. Zum Beweis des Torellischen Satzes. *Nachr. Akad. Wiss. Göttingen. Math.-Phys. Kl. IIa.*, 1957:33–53, 1957. (cited on page 29)

[95] Annegret Weng. Hyperelliptic CM-curves of genus 3. *Journal of the Ramanujan Mathematical Society*, 16(4):339–372, 2001. (cited on page 119)

[96] Annegret Weng. *Konstruktion kryptographisch geeigneter Kurven mit komplexer Multiplikation*. PhD thesis, Institut für Experimentelle Mathematik, Universität GH Essen, 2001. `http://www.uni-due.de/zahlentheorie/theses_de.shtml`. (cited on page 132)

[97] Annegret Weng. Constructing hyperelliptic curves of genus 2 suitable for cryptography. *Mathematics of Computation*, 72(241):435–458, 2002. (cited on pages 41, 43, 70, 120, 124, 157, 162, and 163)

[98] Tonghai Yang. Arithmetic intersection on a Hilbert modular surface and the Faltings height. `http://www.math.wisc.edu/~thyang/RecentPreprint.html`, 2007. (cited on pages 43, 77, 80, 81, and 82)

# List of notation

| | | |
|---|---|---|
| $\backslash$ | this indicates that a large number is continued on the next line | 95 |
| $A(\Phi, \mathfrak{a}, \xi)$ | the principally polarized abelian variety given by $(\mathbf{C}^g/\Phi(\mathfrak{a}), E_{\Phi,\xi})$ | 24 |
| $c$, $c'$, $c''$ | a theta characteristic $c = (c_1, c_2, c_3, c_4)$ is written as $c = (c', c'')$ with $c' = (c_1, c_2)$ and $c'' = (c_3, c_4)$ | 67 |
| $\mathrm{CM}_{F,\Psi}$ | the unramified class field $\mathrm{CM}_{F,\Psi}(1)$ of $F$ generated by complex multiplication | 33 |
| $\mathrm{CM}_{F,\Psi}(\mathfrak{b})$ | a class field of $F$ generated by complex multiplication | 33 |
| $\mathcal{CM}_{K,\Phi}$ | the CM-of-type-$\Phi$ locus in the moduli space of abelian varieties | 92 |
| $\mathcal{CM}_K$ | the CM-by-$K$ locus in the moduli space of abelian varieties | 92 |
| $\Delta$ | the discriminant of $K$ | 39 |
| $\Delta_0$ | the discriminant of $K_0$ | 40 |
| $\Delta_1$ | the norm of the relative discriminant of $K/K_0$, so $\Delta = \Delta_1\Delta_0^2$ | 40 |
| $E$ | a polarization of a complex torus, sometimes short for $E_{\Phi,\xi}$ | 23 |
| $E_{\Phi,\xi}$ | the polarization that is given by the bilinear map $(\Phi(u), \Phi(v)) \mapsto \mathrm{Tr}_{K/\mathbf{Q}}(\xi\overline{u}v)$ | 24 |
| $F$ | a CM-field | 33 |
| $F_0$ | the maximal totally real subfield of $F$ | 33 |
| $h$ | the class number of $K$ | 25 |
| $h'$ | the number of isomorphism classes of principally polarized abelian varieties with CM by a given CM-field | 76 |
| $h_0$ | the class number of $K_0$ | 25 |
| $h_1$ | $h/h_0$ | 25 |

# Index of terms

# Index of people

Numbers with square brackets refer to the bibliography on pages 167–176. Numbers without brackets are a selection of page numbers where the person is mentioned. For more page numbers, see the bibliography.

# Nederlandse samenvatting

## 1 Priemgetallen

De getaltheorie is de studie van de "positieve gehele getallen" 1, 2, 3, 4, ....

Met de "delers" van zo'n getal bedoelen we de positieve gehele getallen waardoor je het kan delen zodat de uitkomst weer een geheel getal is. De delers van 6 zijn bijvoorbeeld $1, 2, 3, 6$. Het getal 4 is geen deler van 6, omdat $6/4 = \frac{3}{2}$ geen geheel getal is.

Als een geheel getal groter dan 1 is, en geen andere delers heeft dan 1 en zichzelf, dan noemen we het getal een "priemgetal". Zo is bijvoorbeeld 5 een priemgetal, want de enige delers van 5 zijn 1 en 5. Het getal 6 is *geen* priemgetal, omdat niet alleen 1 en 6, maar ook 2 en 3 delers van 6 zijn.

Elk positief geheel getal is te krijgen door priemgetallen met elkaar te vermenigvuldigen. Zo is bijvoorbeeld 2010 te schrijven als $2010 = 2 \cdot 3 \cdot 5 \cdot 67$. (We gebruiken hier een punt $(\cdot)$ om vermenigvuldiging aan te duiden.) Het is bekend dat zo'n schrijfwijze voor elk getal uniek is, en in die zin zijn de priemgetallen dus de bouwstenen van de gehele getallen voor vermenigvuldiging.

## 2 Een probleem uit de getaltheorie

Laten we eens een voorbeeld bekijken van een probleem waar een getaltheoreticus zich mee bezig zou kunnen houden.

De *kwadraten* zijn de getallen die te schrijven zijn als een getal maal zichzelf, zoals

$$1 \cdot 1 = 1, \qquad 3 \cdot 3 = 9,$$
$$2 \cdot 2 = 4, \qquad 4 \cdot 4 = 16.$$

Als $a$ een geheel getal is, dan schrijven we vanaf nu voor het gemak $a^2$ in plaats van $a \cdot a$.

Nu kun je je bijvoorbeeld afvragen welke priemgetallen er te krijgen zijn door twee kwadraten bij elkaar op te tellen. Een aantal voorbeelden:

$$2 = 1^2 + 1^2, \qquad 17 = 4^2 + 1^2,$$
$$5 = 2^2 + 1^2, \qquad 29 = 5^2 + 2^2,$$
$$13 = 3^2 + 2^2, \qquad 37 = 6^2 + 1^2.$$

Met de priemgetallen 3, 7, 11, 19, 23 en 31 kan dit niet (probeer maar uit). Zit er een patroon in deze getallen?

# 3 De oplossing

Deel je de bovenstaande priemgetallen door 4 en bekijk je de rest, dan valt er iets op: de priemgetallen 2, 5, 13, 17, 29 en 37, die te schrijven zijn als som van twee kwadraten, hebben allemaal rest 1 of 2, en de priemgetallen 3, 7, 11, 19, 23 en 31, die niet zo te schrijven zijn, hebben allemaal rest 3. Dit patroon blijkt zich voort te zetten en is een wiskundige stelling:

**Stelling 1.** *Gegeven een priemgetal $p$. Als de rest van $p$ bij deling door 4 gelijk is aan 1 of 2, dan is $p$ te krijgen door twee kwadraten bij elkaar op te tellen. Als de rest van $p$ bij deling door 4 niet gelijk is aan 1 of 2, dan is $p$ niet te krijgen door twee kwadraten bij elkaar op te tellen.*

Deze stelling werd in 1640 door de Franse jurist Pierre de Fermat geformuleerd. Het oudste bekende bewijs werd in 1749 gegeven door de Zwitser Leonhard Euler. Men bewijst zo'n stelling niet door heel veel priemgetallen uit te proberen, maar door via een logische beredenering te beargumenteren dat de bewering waar is voor elk priemgetal $p$.

Het geven van zo'n bewijs gaat te ver voor deze samenvatting, maar we kunnen wel het belangrijkste ingrediënt van een modern bewijs noemen: de wortel $i$ van $-1$. Met een "wortel" van een getal $n$ bedoelen we een getal $m$ zodat geldt $m^2 = n$. Het getal 3 is bijvoorbeeld een wortel van 9, want er geldt $3^2 = 9$. Voor $n = -1$ of $n = 2$ bestaat zo'n wortel helemaal niet in de gehele getallen, maar wiskundigen laten zich hierdoor niet tegenhouden en introduceren gewoon een nieuw getal $i = \sqrt{-1}$ waarvoor geldt $i^2 = -1$. Door de gehele getallen uit te breiden met dit soort "algebraïsche getallen" ontstaat het vakgebied van de algebraïsche getaltheorie. We kunnen die getallen ook optellen en vermenigvuldigen en krijgen dan getallen als $3 + 2 \cdot i$.

Voor getallen van de vorm $a + b \cdot \sqrt{-n}$ met gehele getallen $a$, $b$ en $n$, gebruikt men de "norm"

$$a^2 + b^2 \cdot n.$$

Het feit dat het priemgetal 13 te schrijven is als som van de twee kwadraten $3^2$ en $2^2$ correspondeert zo met het feit dat 13 de norm is van $3 + 2 \cdot i$. Met wat meer werk kan je getallen als $3 + 2 \cdot i$ gebruiken om Stelling 1 te bewijzen.

# 4 Een variant op het probleem

Wat nu als we willen weten welke priemgetallen te schrijven zijn als een kwadraat plus 2 maal een kwadraat? Zo hebben we

$$3 = 1^2 + 2 \cdot 1^2, \qquad 17 = 3^2 + 2 \cdot 2^2,$$
$$11 = 3^2 + 2 \cdot 1^2, \qquad 19 = 1^2 + 2 \cdot 3^2,$$

maar zijn de getallen 5, 7, 13 en 23 *niet* zo te schrijven.

Voor dit probleem kijken we eenvoudigweg naar een wortel van $-2$, die we schrijven als $\sqrt{-2}$. Het bewijs van Stelling 1 (dat we niet gegeven hebben) blijkt te veralgemeniseren te zijn en levert een soortgelijke stelling op:

**Stelling 2** (Euler)**.** *Gegeven een priemgetal $p$. Als de rest van $p$ bij deling door 8 gelijk is aan 1, 2 of 3, dan is $p$ te schrijven als som van een kwadraat en 2 maal een kwadraat. Als de rest van $p$ bij deling door 8 niet gelijk is aan 1, 2 of 3, dan is $p$ niet zo te schrijven.*

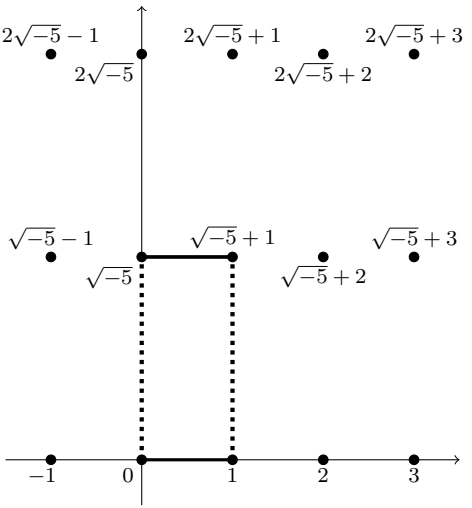
Vervolgens kan je je afvragen welke priemgetallen te schrijven zijn als een kwadraat plus 3 maal een kwadraat, of als een kwadraat plus 4 maal een kwadraat. Dat kan allemaal met ongeveer hetzelfde bewijs, gebruikmakend van de wortel van $-3$ of juist van $-4$.

Maar bij 5 gaat het mis! Als je op de manier van Stellingen 1 en 2 wilt zeggen welke priemgetallen er te schrijven zijn als een kwadraat plus 5 maal een kwadraat, dan blijkt dat je niet meer genoeg hebt aan alleen de wortel van $-5$. Gelukkig blijkt er toch een enigszins soortgelijke stelling te bestaan, maar voor het bewijs daarvoor gebruikt men naast de wortel van $-5$ opeens ook de wortel van 5.

Als je de 5 vervangt door nog grotere getallen $n$, dan heb je vaak nog veel ingewikkeldere algebraïsche getallen nodig dan de wortel van 5. Welke, daar kun je achter komen met de theorie van de "complexe vermenigvuldiging van elliptische krommen". Dit is de "complex multiplication" die ook in de titel van dit proefschrift voorkomt.

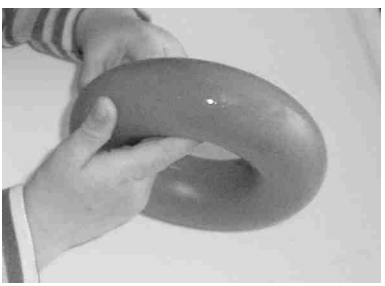
# 5 Fietsbanden

In plaats van de lijn van de reële getallen, maken we gebruik van het vlak van de "complexe getallen". De reële getallen vormen daarin een horizontale lijn, en een getal $\sqrt{-n}$ leggen we recht boven de 0 op afstand $\sqrt{n}$ van 0, zoals in het volgende plaatje.

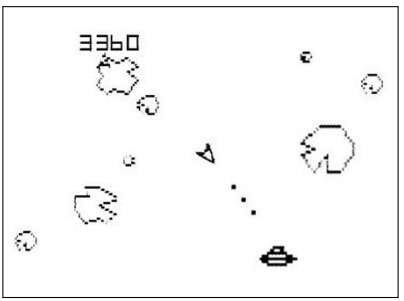



In dit vlak hebben we een rechthoek aangegeven. Stel nu dat je deze rechthoek uitknipt en langs de stippellijnen aan zichzelf plakt. Je krijgt dan een soort wc-rolletje.

Als dat wc-rolletje flexibel genoeg is, dan kan je ook de dikke lijnen aan elkaar plakken. Wat je dan krijgt, lijkt nog het meest op een fietsband. Buiten Nederland zouden we zeggen: het oppervlak van een donut. Stel dat je een donut volledig bedekt met glazuur. De vorm van ons geplakte rechthoekje is dan dezelfde als de vorm van het glazuur van de donut. Wiskundigen noemen dit oppervlak een *torus*.



Een torus.




Asteroids.

In zekere zin plakken wiskundigen de randen van de rechthoek aan elkaar *zonder* hem te buigen, precies zoals bij het computerspelletje *Asteroids*: daarbij speel je op een plat vlak, maar alles wat aan de zijkant het beeld uitgaat, verschijnt weer aan de andere zijkant, en hetzelfde geldt voor de boven- en onderkant.

# 6 Elliptische krommen

We noemen de verzameling oplossingen $(x, y)$ van een vergelijking van de vorm

$$y^2 = x^3 + ax + b \tag{6.1}$$

voor zekere getallen $a$ en $b$, een "elliptische kromme".

Als we kijken naar de *reële* oplossingen, dan kunnen we deze kromme tekenen in het vlak met coördinaten $x$ en $y$. Dat levert dan een plaatje op als op pagina 9.

Als we de *lijn* van de reële getallen vervangen door het *vlak* van de complexe getallen, dan is de oplossingsverzameling geen kromme, maar een *oppervlak*. En als we er op de juiste manier naar kijken, dan blijkt dit oppervlak ook weer de vorm van een torus te hebben.

Het omgekeerde is ook waar: elke torus die we krijgen door een rechthoekje van complexe getallen te plakken is (binnen de regels van de "complexe analyse") om te vormen tot een elliptische kromme!

Er blijkt nog meer waar te zijn: als je begint met de rechthoek die hoort bij een getal $\sqrt{-n}$, dan kan de genoemde vervorming zo uitgevoerd worden dat de getallen $a$ en $b$ niet zomaar complexe getallen zijn, maar *algebraïsche* getallen.

In het geval $n = 5$ krijg je bijvoorbeeld

$$a = b = \frac{4420 \cdot \sqrt{5} + 9875}{27}.$$

Merk de wortel $\sqrt{5}$ van 5 op, die een rol speelt in de oplossing van het getaltheorieprobleem. Dat uitgerekend dat getal $\sqrt{5}$ hier voorkomt is geen toeval: dat kan verklaard worden met de theorie van complexe vermenigvuldiging van elliptische krommen.

We kunnen dat preciezer maken met behulp van de "$j$-invariant"

$$j = \frac{110592a^3}{64a^3 + 432b^2},$$

die aangeeft wanneer twee elliptische krommen in zekere zin "hetzelfde" zijn. Twee elliptische krommen zijn hetzelfde als ze dezelfde $j$-invariant hebben.

Door het bestuderen van de relevante vervormingen, heeft men formules gevonden die de $j$-invariant rechtstreeks uitdrukken in ons complexe getal $z = \sqrt{-n}$, dat de bovenkant van de rechthoek aangeeft. De exacte betekenis van de formules is voor deze samenvatting niet belangrijk, ze staan hier enkel ter illustratie:

$$j(z) = 256\frac{(\theta_0^8 - \theta_0^4\theta_1^4 + \theta_1^8)^3}{\theta_0^8\theta_1^8(\theta_0^4 - \theta_1^4)^2}, \qquad \text{met}$$

$$\theta_0 = 1 + 2\sum_{n=1}^{\infty} q^{\frac{1}{2}n^2},$$

$$\theta_1 = 1 + 2\sum_{n=1}^{\infty} (-1)^n q^{\frac{1}{2}n^2} \qquad \text{en}$$

$$q = e^{2\pi i z}$$

Het symbool $\infty$ in deze formules betekent "oneindig" en geeft aan dat we oneindig veel, steeds kleinere, getallen bij elkaar optellen. We kunnen met deze formule de $j$-invariant dus niet uitrekenen op een computer, maar wel *benaderen* door hem gedeeltelijk uit te rekenen. Met behulp van wiskundige theorie kunnen we exact maken hoe ver we $j(z)$ moeten benaderen om de exacte waarde te kennen. Er blijkt dat geldt

$$j(\sqrt{-5}) = 632000 + 282880\sqrt{5},$$

met wederom die wortel van 5.

Als we onze $-5$ nu vervangen door een ander negatief geheel getal $-n$, dan kunnen we de $j$-invariant $j(\sqrt{-n})$ bekijken. Volgens de theorie van complexe vermenigvuldiging is dit precies het getal dat we, naast $\sqrt{-n}$, moeten toevoegen om stellingen te krijgen over priemgetallen van de vorm $a^2 + nb^2$. Als je wilt weten welke priemgetallen te schrijven zijn als kwadraat plus 14 maal een kwadraat, dan kan je bijvoorbeeld gebruik maken van

$$\begin{aligned} j(\sqrt{-14}) =& 4055096128 + 2867386368\sqrt{2} + \\ & 1792\sqrt{10241006292718 + 7241484995756\sqrt{2}}. \end{aligned}$$

De geïnteresseerde wiskundige lezer kan hier veel meer over lezen in het zeer toegankelijke boek [19] van David A. Cox.

# 7 Pinpassen en slimme prijskaartjes

Een heel ander soort toepassing van elliptische krommen vindt men in de *cryptografie*, waarbij gegevens of elektronische systemen worden be-

veiligd met behulp van wiskunde. Deze beveiliging is erop gebaseerd dat sommige berekeningen eenvoudig uit te voeren, maar moeilijk terug te draaien zijn. Zo kan je met een computer heel snel twee grote priemgetallen $p$ en $q$ met elkaar vermenigvuldigen. De uitkomst is dan een groot getal $N$ en ondanks decennia van onderzoek is er nog geen snelle manier bekend om achter $p$ en $q$ te komen als je alleen $N$ weet.

Tegenwoordig worden de magneetstrips van bankpasjes op vrij grote schaal gekopieerd door criminelen die betaalautomaten ombouwen. De oplossing daarvoor is op de meeste passen al aanwezig in de vorm van de EMV-chip. Die chip bevat twee priemgetallen die alleen in de chip beschikbaar zijn. Bij elke betaling kan je bankpasje dankzij het "RSA-protocol" bewijzen dat het echt jouw bankpasje is. De chip gebruikt daarvoor de priemgetallen $p$ en $q$ zonder ze te verraden. Dit maakt het (met de huidige stand van de wetenschap) onmogelijk om de chips van deze passen te kopiëren.

De laatste tijd worden ook passen die op afstand leesbaar zijn steeds populairder. Denk aan de OV-chipkaart die je niet meer uit je portemonnee hoeft te halen, je paspoort waar je foto en vingerafdruk op zijn opgeslagen, en misschien wel de pas waarmee je het kantoor in en uit kan. Verder wordt het steeds meer mogelijk om streepjescodes in bijvoorbeeld winkels, apotheken en magazijnen te vervangen door goedkope chips die RFID-tags heten.

Doordat deze pasjes en RFID-tags op afstand uit te lezen zijn, zijn er veel veiligheids- en privacyrisico's. Goede beveiliging is dus belangrijk.

Aan de andere kant hebben juist deze passen veel minder energie tot hun beschikking dan bijvoorbeeld de chip op een bankpasje. Er is namelijk geen plaats voor een batterij en ze kunnen ook geen contact maken met netstroom. Ze moeten al hun energie daarom via een kleine antenne uit het magnetische veld van het leesapparaat halen.

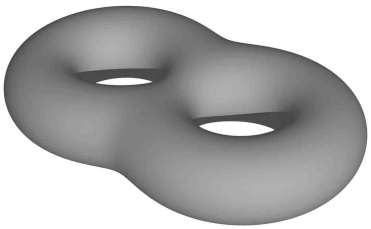
Door de beperkte hoeveelheid energie is een RFID-tag niet in staat het RSA-protocol van je bankpasje uit te voeren. Hier bieden elliptische krommen, die we hierboven al tegenkwamen, uitkomst.

Er bestaat namelijk ook cryptografie die gebruik maakt van elliptische krommen. Die biedt, voor zover bekend, evenveel veiligheid als RSA met veel lichtere berekeningen. Cryptografie met elliptische krommen kan *wel* op RFID-tags uitgevoerd worden.

Om elliptische krommen te maken die geschikt zijn voor cryptografie, kan je gebruik maken van dezelfde theorie van "complexe vermenigvuldiging" die eerder al genoemd werd. Daarbij gebruikt men dezelfde speciale waarden van de $j$-functie die we hierboven al tegenkwamen.

# 8 Dubbele donuts

Dit proefschrift gaat niet over elliptische krommen, maar over krommen van geslacht 2. Denk even terug aan de donuts. Stel nu dat twee donuts iets te dicht bij elkaar hebben gelegen op de bakplaat en daardoor aan elkaar geplakt zijn. En stel nu dat we deze dubbele donut volledig met glazuur bedekken. Het glazuur vormt dan wat we noemen een *dubbele torus*, eentje met twee handvatten, zoals op het volgende plaatje.



Vergelijking (6.1) wordt dan vervangen door

$$y^2 = x^6 + ax^4 + bx^3 + cx^2 + dx + e$$

voor zekere getallen $a$, $b$, $c$, $d$ en $e$. Daarbij hoort het plaatje op pagina 12, maar ook het plaatje op de omslag.

Met een aantal wijzigingen bestaat er dan nog steeds een theorie van complexe vermenigvuldiging. Daarin moet bijvoorbeeld de $j$-invariant vervangen worden door drie invarianten die *Igusa-invarianten* heten.

Je kunt je nu afvragen of er met deze krommen ook getaltheoretische vraagstukken opgelost kunnen worden. Tegelijkertijd bestaat er ook cryptografie met krommen van geslacht 2. Daarmee is ongeveer hetzelfde mogelijk als met elliptische krommen, en het is nog maar de vraag welke krommen het "best" zijn.

# 9 Wat staat er in dit proefschrift?

In dit proefschrift wordt de theorie van complexe vermenigvuldiging van krommen van geslacht 2 bestudeerd en zo expliciet mogelijk gemaakt, zodat er berekeningen mee gedaan kunnen worden.

Hoofdstuk I geeft een algemene inleiding in de theorie van complexe vermenigvuldiging. Vervolgens wordt in dat hoofdstuk door middel van "klassenlichamentheorie" beschreven welke soorten getaltheoretische problemen kunnen worden opgelost met behulp van complexe vermenigvuldiging van krommen van geslacht 2.

Hoofdstuk II beschrijft hoe je de exacte waarden van de bovengenoemde Igusa-invarianten krijgt. Dat wil zeggen, er wordt beschreven en hoe, en hoe nauwkeurig, je ze moet benaderen om ze exact te bepalen. Het belangrijkste resultaat van dit (langste) hoofdstuk is een bovengrens op hoe lang deze berekeningen duren.

Hoofdstuk III geeft nog wat extra theorie en wijst belangrijke verbeteringen aan voor de berekeningen van hoofdstuk II. Die verbeteringen zijn weggelaten in hoofdstuk II, omdat dat hoofdstuk al lang genoeg is.

Hoofdstuk IV, geschreven samen met David Freeman en Peter Stevenhagen, beschrijft hoe je de Igusa-invarianten gebruikt om krommen te maken die geschikt zijn voor cryptografische protocollen gebaseerd op "bilineaire afbeeldingen".

Hoofdstuk V, geschreven met Laura Hitt, Gary McGuire en Michael Naehrig, beschrijft een soortgelijke constructie, maar dan voor een speciaal soort krommen van geslacht 2: die waarvan de $p$-rang, een invariant die voor alle eerdere constructies 0 of 2 is, gelijk is aan 1.

# Dankwoord / Acknowledgements

Op deze pagina wil ik graag kort een aantal mensen bedanken die betrokken zijn bij de totstandkoming van dit proefschrift. Als eerste mijn vrouw, Marina, voor al haar steun, vooral tijdens de drukke laatste weken.

Mijn kantoorgenoot, Peter Bruin, voor vier jaar geduldig luisteren naar mijn onderbrekingen en vragen over meetkunde.

Mijn promotor, Peter Stevenhagen, zonder wiens gedetailleerde commentaar dit proefschrift niet zou zijn wat het nu is. En naast hem ook mijn andere co-auteur van hoofdstuk IV, David Freeman, die inmiddels voldoende Nederlands leest om dit te begrijpen: bedankt voor de goede samenwerking.

Nu zal ik helaas toch op het Engels over moeten gaan. Thanks also to my co-authors Laura Hitt, Gary McGuire, and Michael Naehrig for the collaboration on Chapter V.

Thank you Andreas Enge for inviting me to Bordeaux, and for your hospitality and our inspiring collaboration.

Thank you Jens Putzka for the same things, with Bonn instead of Bordeaux.

Thank you Kristin Lauter for letting me be your intern at Microsoft Research, and for your hospitality and our collaboration. Reinier Bröker, die laatste dingen gelden natuurlijk ook voor jou, maar dan in het Nederlands.

Finally, thanks to everyone who gave suggestions and corrections for the improvement of the manuscript, including Reinier Bröker, Andreas Enge, David Freeman, and the members of the committee.

# Curriculum vitae

Marco Streng werd geboren op 26 november 1982 in IJsselstein. Hij verhuisde al snel naar Benschop, waar hij meer dan de helft van zijn leven tot nu toe heeft gewoond. Na de basisschool ging hij naar het VWO van het Cals College in IJsselstein en Nieuwegein.

In 2001 begon hij zijn studie wiskunde aan de Universiteit Utrecht. In de eerste jaren volgde hij daarnaast ook vakken bij natuurkunde en informatica en haalde hij een propedeusediploma in de informatica. Onder begeleiding van dr. Gunther Cornelissen schreef hij zijn afstudeerscriptie *Elliptic Divisibility Sequences with Complex Multiplication*, waarop hij in 2006 cum laude afstudeerde in de wiskunde.

Vervolgens begon hij als promovendus aan het Mathematisch Instituut van de Universiteit Leiden. Het promotieonderzoek werd gedaan onder begeleiding van prof. dr. Peter Stevenhagen. Naast zijn promotieonderzoek was Marco werkzaam in het wiskundeonderwijs van de universiteit. Verder heeft hij gedurende 11 weken in het najaar van 2008 als stagiair onderzoek gedaan in de cryptografiegroep van Microsoft Research in Redmond in de Verenigde Staten.

Sinds 20 augustus 2008 is hij gehuwd met Marina Blokland, en op 11 april 2009 werden zij de trotse ouders van Tijmen. Hun tweede zoon wordt in juli 2010 verwacht.

Per 1 september 2010 is Marco als Research Fellow verbonden aan de University of Warwick.